2018 Issue 1 // Volume 114

THE BRIDGE

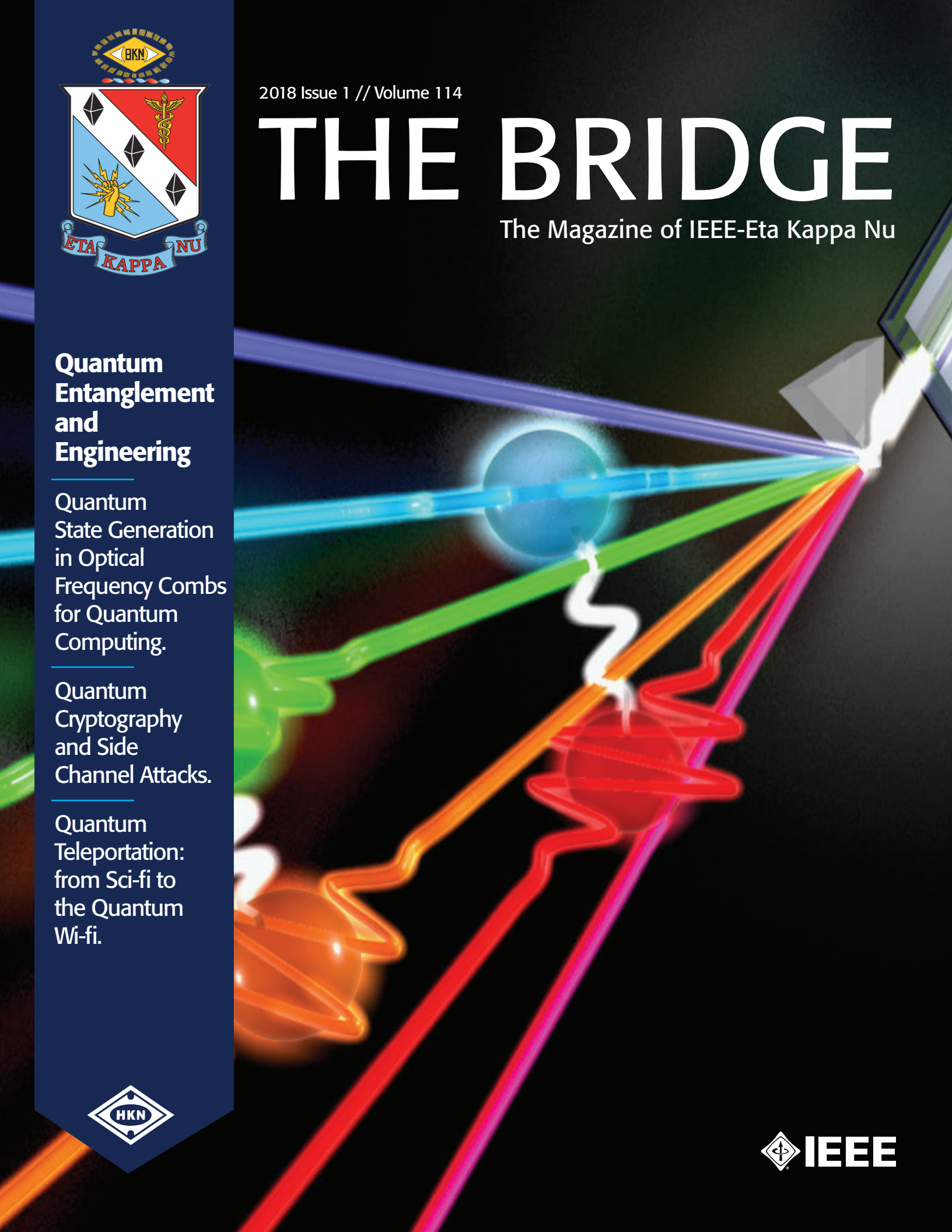
The Magazine of IEEE-Eta Kappa Nu

Quantum Entanglement and Engineering

Quantum State Generation in Optical Frequency Combs for Quantum Computing.

Quantum Cryptography and Side Channel Attacks.

Quantum Teleportation: from Sci-fi to the Quantum Wi-fi.



IEEE-HKN AWARD PROGRAM

As the Honor Society of IEEE, IEEE-Eta Kappa Nu provides opportunities to promote and encourage outstanding students, educators and members.

Visit our new website to view the awards programs, awards committees, list of past winners, nomination criteria and deadlines.

ALTON B. ZERBY AND CARL T. KOERNER OUTSTANDING STUDENT AWARD (OSA)

Presented annually to a senior who has proven outstanding scholastic excellence and high moral character, and has demonstrated exemplary service to classmates, university, community, and country.
(Deadline: 30 June)

C. HOLMES MACDONALD OUTSTANDING TEACHING AWARD (OTA)

Presented annually to electrical engineering professors who have demonstrated, early in their careers, special dedication and creativity in their teaching, as well as a balance between pressure for research and publications.
(Deadline: Monday after 30 April)

DISTINGUISHED SERVICE AWARD

Recognizes members who have devoted years of service and lifetime contributions to Eta Kappa Nu (or IEEE-HKN), resulting in significant benefits to all of the Society's members.
(Deadline: Monday after 30 April)

OUTSTANDING CHAPTER AWARD (OCA)

Recognizes chapters for excellence in activities and service at the department, university and community levels. The award is based on the content contained in their Annual Chapter Report for the preceding academic year.
(Deadline: Monday after 30 September)

OUTSTANDING YOUNG PROFESSIONAL AWARD (OYP)

Presented annually to an exceptional young engineer who has demonstrated significant contributions early in their professional career.
(Deadline: Monday after 30 April)

VLADIMIR KARAPETOFF OUTSTANDING TECHNICAL ACHIEVEMENT AWARD

Recognizes individuals who have distinguished themselves through an invention, development, or discovery in the field of electrical or computer engineering.
(Deadline: Monday after 30 April)

IEEE-Eta Kappa Nu Board of Governors

IEEE-Eta Kappa Nu (IEEE-HKN) was founded by Maurice L. Carr at the University of Illinois at Urbana- Champaign on 28 October 1904, to encourage excellence in education for the benefit of the public. IEEE-HKN fosters excellence by recognizing those students and professionals who have conferred honor upon engineering education through distinguished scholarship, activities, leadership, and exemplary character as students in electrical or computer engineering, or by their professional attainments. THE BRIDGE is the official publication of IEEE-HKN. Ideas and opinions expressed in THE BRIDGE are those of the individuals and do not necessarily represent the views of IEEE-HKN, the Board of Governors, or the magazine staff.

Get in touch with Eta Kappa Nu Twitter: ieee_etakappanu Facebook: IEEE-HKN

Cover image: "On-chip non classical frequency combs for complex quantum state generation", Credit: Michael Kues/UOP Group

THE BRIDGE

The Magazine of IEEE-Eta Kappa Nu

ISSUE 1, 2018 — Quantum Entanglement and Engineering

Features

Departments

IEEE-HKN INTERNATIONAL HEADQUARTERS
Editorial inquiries: IEEE- Eta Kappa Nu, 445 Hoes Lane, Piscataway, NJ 08854, USA
US Toll Free: +1 800 406 2590 | Outside US: +1 732 465 5846
Email: info@hkn.org | www.hkn.org

Subscription address and email changes: IEEE Contact Center
US Toll Free: +1 800 678 4333 | Outside US: +1 732 981 0060 | Fax: +1 732 562 6380 | Email: contactcenter@ieee.org

Letter from the President and Director

Steve Watkins

President
Gamma Theta Chapter
steve.e.watkins@ieee.org

Nancy Ostin

Director
Gamma Theta Chapter
n.ostin@ieee.org

Dear Eta Kappa Nu (HKN) Members and Friends

HKN and IEEE-HKN has a distinguished history and membership. It has done much to promote excellence in the profession and in education through its emphasis on scholarship, character, and service. The Wheatstone bridge emblem represents the "balanced life" as described in the induction ritual is represented aptly. When you use this emblem, you are showing your connection to more than 200,000 members worldwide.

The organization is healthy with nearly 3,000 new members inducted, 11 chapters chartered or reinstated, and a new website launched last year. The 217 active chapters continue to provide thousands of service hours to their institutions and communities. We thank 2017 President Tim Kurzweg and his leadership team for outstanding work. During the beginning of 2018, we are already seeing notable activity among the chapters, committees, and leadership. In particular, the current Board of Governors is giving special emphasis to our financial resources, faculty advisor support, the student conference, branding, and the chapter experience.

The broad impact of IEEE-HKN is evident from the chapter reports. Departments benefit through tutoring and mentoring activities; communities benefit from service and STEM outreach, and new chapters benefit from mentoring by established chapters. The positive influence of HKN experiences are obvious as we talk with both students, faculty, and working engineers. This quote from a student is one of our favorites:

> "HKN has fundamentally changed the way I lead as a leader (for the better) and challenged me, persistently, to be a better engineer, friend, and person."

A Wheatstone Bridge Membership Plaque

As we nurture the next generation of engineers who will change our world, thank you for joining us on the journey. To our alumni and supporters, Faculty Advisors and Department Heads, chapter officers and members, thank you for all you do on behalf of Eta Kappa Nu.

We welcome the 2018 leadership team especially our new members of the Board of Governors and our new Editors-in Chief – Drs. Sahra Sedigh and Stephen Williams. In addition, we think you will enjoy this issue of THE BRIDGE which was coordinated by guest editor and new board member Dr. Sean Bentley.

Regards,

Steve E. Watkins

Steve E. Watkins

Nancy Ostin

Nancy Ostin

Student Collaboration

Hello HKN! We are Michael Benson and Katie Lewis, your TWO HKN student governors for 2018. We're thrilled to work together with you this year and we're excited and honored to serve you for the 2018 calendar year.

If you're a chapter officer, you've likely already heard from one of us by now. If you haven't, please don't hesitate to contact us… some of our chapters don't have the most up-to-date contact information on file. (PSA: Chapters, please be sure to update your contact information regularly!) One of our main objectives this year is to increase the communication and sharing of best practices between chapters. In addition to continuing the monthly chapter leader meetings, we will be launching some new initiatives to help bolster the resources available to you.

We are especially looking forward to working with each of you (alumni and undergraduates alike) to find creative ways to keep our members (YOU) involved past graduation. Our society has a wealth of experience and we're barely scratching the surface of our potential at this point. We both feel strongly that strong chapters have strong alumni engagement. We'd like to ask you to consider engaging with your chapter of induction or even a local chapter as an advisor, mentor, or donor. If this is something that you're passionate about too, please reach out to one of us!

Finally, and perhaps most importantly, we're excited to be representing some of the best and brightest students in the world. Working with the other members of the Board, we're going to ensure that Eta Kappa Nu serves your needs, serves our communities, and is a true mark of distinction.

Michael Benson

2018 HKN Student Governor
Beta Epsilon Chapter

Katie Lewis

2018 HKN Student Governor
Kappa Sigma Chapter

Sean J. Bentley
IEEE-HKN Board
of Governors
Guest Editor
Gamma Theta Chapter

Quantum Entanglement: Engineering the Future

Four years ago, I wrote an article in The Bridge talking about the coming importance of quantum entanglement for electrical engineering applications. While not a Nostradamus-like prediction as commercialization was well under way at that time, activity and corporate involvement in these areas have exploded recently.

The Quantum Computing for Business (Q2B) conference was held at NASA-Ames Research Center in early December, 2017. The conference not only drew companies developing the technology, but also companies such as VW, Goldman Sachs, and Airbus, with plans to apply quantum computing to a wide variety of industries. D-Wave, the first company to have commercially available quantum computers, has deployed their equipment into several major research efforts including artificial intelligence. Technology giants Google and IBM are currently battling for the lead in the race for the most powerful quantum computer. Both public and private funding for quantum computing research around the world has increased dramatically in the past few years.

Quantum cryptographic systems have now been in use at various levels for over a decade, though much progress continues to be made. There are still concerns with possible security vulnerabilities (with one discussed in this issue), speed, and widespread implementation. Thus, most systems continue to use more traditional cryptographic methods, but with the reality of quantum computers looming and their predicted ability to defeat such classical systems, the government is determined to perfect quantum cryptography sooner than later.

Modern electrical and computer engineering have long been based heavily in two quantum-based technologies, the transistor and the laser. Because of this, electrical engineering students have long been required to take at least a modern physics course, where you learn some basics of quantum mechanics, including properties referred to by many as "quantum weirdness." Most of these weird properties can be accepted easily, though, if you are willing to accept that massive particles such as electrons can have wavelike properties. The uncertainty principle is essentially nothing more than a Fourier transform diffraction limit. Tunneling is completely analogous to evanescent coupling used in optics and electromagnetics. Entanglement, however, is a whole new ballgame.

Quantum entanglement is the property linking two (or more) particles with properties that can only be described jointly, going far beyond any classical correlation, and existing simultaneously across multiple bases. Entanglement first came to light in the now-famous 1935 EPR paper in which Einstein and colleagues used it to try to explain why quantum mechanics was an incomplete theory. At that time, however, not only was there no experimental way to generate such particles, there was also not a theoretical way to differentiate Einstein's claims from those of quantum theory. In the 1950s, John Bell developed a formalism that could distinguish the two viewpoints, but experimental techniques had still not caught up. Finally, in the early 1970s John Clauser performed the first experiment to show that indeed quantum mechanics was correct (and this has since been verified by experiment after experiment, continually becoming more precise and more free of interpretive loopholes; I personally had the honor in the early 2000s of being a part of the team that finally did the experiment directly as envisioned in the original EPR paper). Now that entanglement is widely accepted and relatively easy to achieve in the laboratory, its "spooky" properties have opened up a wide variety of applications, including imaging, communications, computing, cryptography, and more.

The goal of this issue is to get you excited about the importance of quantum entanglement to the future of technology and electrical engineering, possibly prompting some of you to get involved in these areas. The articles introduce some of the basics of quantum entanglement and a few of the technologies stemming from it. The first paper discusses some of the current practical challenges to quantum computers, along with a possible solution using another key technology, frequency combs. The second paper discusses the theory and reality of quantum cryptography, and addresses a possible real-world challenge that needs to be considered. Finally, the last paper gives an introduction to quantum teleportation, showing that it is not only reality, but also the basis for many of the other technologies. Enjoy this glimpse into the world of quantum entanglement, and hopefully many of you will join the effort of engineering the future.

Sean J. Bentley earned his BSEE ('95) and MSEE ('97) from the University of Missouri-Rolla (now Missouri University of Science and Technology), and his Ph.D. in Optics ('04) from the University of Rochester. He is an Associate Professor of Physics at Adelphi University, where he was awarded the Teaching Excellence Award for 2012-13. From 2014-2016, he served as Director of the Society of Physics Students and Sigma Pi Sigma (the physics honor society) at the American Institute of Physics. He is authoring a text on quantum imaging and holds a patent in nonlinear lithography. He is a member of the IEEE Photonic Society, and was elected to membership in IEEE-HKN as an undergraduate.

Quantum State Generation in Optical Frequency Combs for Quantum Computing

by: Yanbing Zhang, Piotr Roztocki, Christian Reimer, Stefania Sciara, Michael Kues, David J. Moss, and Roberto Morandotti

Key words: optical frequency combs, integrated quantum sources, high-dimensional quantum states.

Quantum states represent a key resource for quantum computing, with the potential to advance practical implementations beyond proof of concept demonstrations. Optical frequency combs (broadband light sources spanning a large bandwidth of equidistantly-spaced spectral lines, which were first developed for classical optical applications), are a promising approach to generate the required quantum states. The advantages of quantum frequency combs have been supported by the development and application of quantum photonic sources in both bulk systems and integrated platforms. In combination with the benefits of integrated photonics, which is increasingly perceived as a practical, scalable platform for implementing quantum technology, integrated quantum frequency combs allow the generation of scalable, complex quantum states in a low-cost and ultra-compact footprint, as well as their manipulation using standard telecommunications signal processing techniques.

INTRODUCTION

In the last few decades, research towards achieving the holy grail of universal quantum computers has greatly intensified, with the promise of being able to perform calculations that are completely beyond the capability of conventional electronic computers. To implement a quantum computer, a physical system is required that can support the preparation, manipulation, and measurement of quantum bits (qubits), units of quantum information analogous to classical bits. Since quantum states are so delicate that their surroundings can quickly deteriorate the quantum information, the host media should be capable of shielding them from the outside environment [1]. Also, the physical qubits should be scalable and able to be precisely controlled in order to realize a universal set of quantum logic gates [2]. Furthermore, the errors induced in these qubits due to inevitable disturbances need to be effectively corrected during operations to preserve the quantum information. Quantum technologies are being advanced in several platforms including electronic, ions, solid state, nuclear magnetic resonance, and superconducting systems [1].

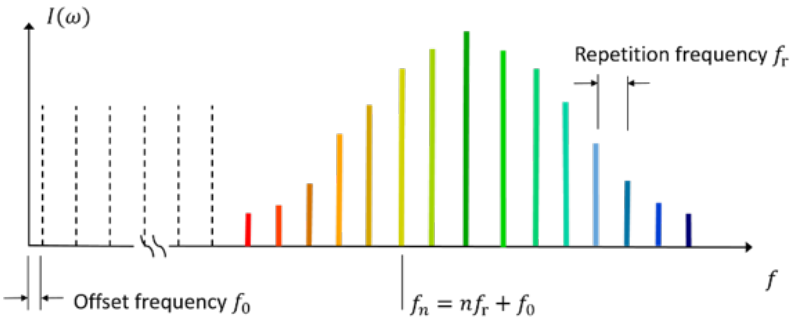


Fig.1 Schematic of a classical optical frequency comb, which consists of a series of discrete, equally-spaced frequency lines. The comb may function as a frequency ruler since unknown frequencies can be measured relative to a precisely known n-th order frequency (f_n), with the offset frequency (f_o) and the repetition frequency (f_r) known and stabilized.

Photons are one of the best candidates for quantum system realizations. They exhibit very low decoherence, which improves the capability to preserve the quantum states sufficiently long enough to perform an operation. Qubits can easily be encoded in a photon via their different degrees

of freedom, such as polarization, path, frequency, time, and angular momentum [2]. In addition, photon-based qubits are compatible with the well-established telecommunications infrastructure, and exhibit excellent transmission in fiber optics. However, large and intricate optical quantum states, which are a key cornerstone for realizing optical quantum computers, remain difficult to prepare and entangle.

Optical frequency combs - broadband optical sources that have equidistantly-spaced coherent spectral lines – (Fig. 1) provide an elegant solution to this issue. Due to the lines' precise spectral locations, frequency combs have served as extremely precise optical rulers, enabling a revolution in high-precision metrology and spectroscopy [3]. Recently, the classical frequency comb concept has been extended to the quantum world for the preparation of quantum states. This approach brings about many benefits, especially for the creation of large quantum states. First, frequency combs offer many experimentally-accessible frequency modes within a single spatial mode, where all the photons of different wavelengths are transmitted together in a single waveguide. Furthermore, the intrinsic multi-frequency-mode characteristics enable the generation of many entangled quantum states simultaneously, with the density of these quantum channels controllable via the spectral mode separation. Finally, the frequency domain is complementary to other degrees of freedom, enabling the creation of even larger-scale quantum states. Many approaches to quantum state preparation use quantum frequency combs, such as for the generation of heralded single photons [4-9], as well as two-photon entangled states via the time [10-13], energy [14-16], path [17] and frequency [18] degrees of freedom. In addition, large and complex states, e.g. high-dimensional (quDit) entangled states [19-21], cluster states [22-24], and multipartite entanglement [25, 26], have been predicted and achieved for applications in quantum signal processing, including quantum logic gates [21], boson sampling [27], and spectral linear optical quantum computation [28].

QUANTUM FREQUENCY COMB IN BULK SYSTEMS

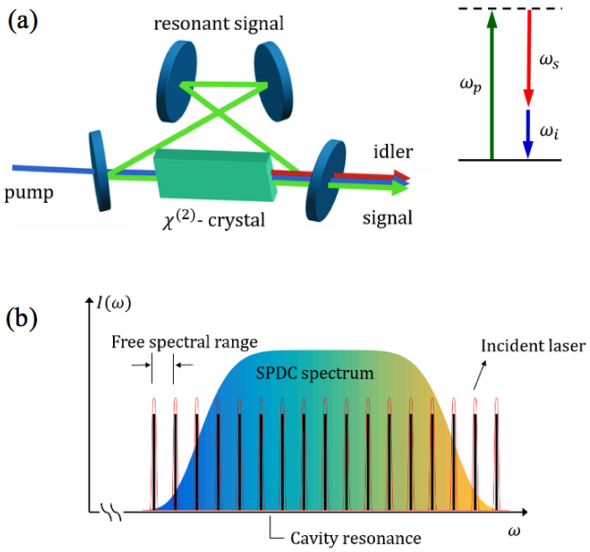


Fig.2 Schematic of quantum frequency comb generation in free space optics. (a) Inside an optical parametric oscillator (where part of the figure is adapted from [29]), a second-order $\chi^{(2)}$- nonlinear crystal converts the input pump beam at frequency (ω_p) into output signal and idler beams at frequencies (ω_i, ω_s) through spontaneous parametric down-conversion (SPDC), satisfying the relation ($\omega_i+\omega_s=\omega_p$). (b) The quantum frequency comb is generated on the intra-cavity resonances by spectrally filtering the broadband SPDC spectrum. When the input pump is a pulse train, the incident pulse spectrum (solid lines) has to match perfectly with the cavity resonances (solid bars), separated by one free spectral range (FSR) [30].

The first investigations of quantum frequency combs were based on bulk free-space setups, exploiting spontaneous parametric down-conversion (SPDC). In this approach, an optical parametric oscillator (OPO) in a 2nd order nonlinear crystal, such as PPKTP [24] or BBO [30], is operated below the OPO threshold. In this process, a high-energy pump photon splits into a pair of lower-energy

photons (signal and idler) satisfying both energy conservation and the imposed cavity resonance conditions (see Fig. 2). In cases where the nonlinear crystal has a large phase-matching bandwidth, a broadband quantum frequency comb of entangled photon pairs is created by the OPO at the resonant wavelengths. This process was predicted to exhibit multi-partite entanglement [31] and multi-qubit entanglement [32], and this was quickly realised experimentally [24], showing that it indeed has the potential for generating large-scale quantum states. In particular, each cavity mode of a frequency comb can be described by a quantum harmonic oscillator and, analogous to the position and momentum observables, the field's continuous-variable Hilbert space can be described by its amplitude or phase-quadrature observables. This approach has been used to generate continuous-variable non-classical states based on squeezed light, where the noise of one quadrature of the electrical field is below the optical shot noise. Since these quantum sources can be operated by using well-known opto-electronic modulation and homodyne techniques [33], they allow for deterministic quantum operations. Moreover, the squeezing property, controlled by phase-sensitive nonlinear gain, has been used effectively to generate single-mode squeezed vacuum states [33], and theoretical work predicts that they can potentially provide qubit-like behaviour around the oscillation threshold [34].

In continuous-wave (CW) pumped schemes, quantum state preparation using squeezed states has been remarkably successful. Examples include the generation of many complex states with, for example, the simultaneous generation of 15 quadripartite entangled quantum states using 60 cavity modes [24], or the generation of one 60-mode and two 30-mode copies of a dual-rail quantum-wire state [25]. Richer excitation spectra and more tailored nonlinear optical interactions have been predicted to enable larger states [24], and even in the latter experiments the mode number was limited by measurement capability, rather than by the actual generation, with the maximum number of entangled modes predicted to be at least 6700 [25]. When the OPO is pumped by a pulse train, these photon pairs become interlinked through the introduction of frequency correlations beyond purely symmetric pair creation. The injection of a femtosecond pulse train with individual frequency modes into the cavity can induce an intimate connection between symmetric and asymmetric frequency correlations [35]. Through the control of the nonlinear crystal, the optical cavity, and the pulse characteristics, such a system was used to realize quantum networks with a total of 511 possible entangled bipartitions among 10 spectral regions [30]. A follow-up experiment demonstrated the first full multipartite entanglement with an entangled state for all of the 115,974 possible nontrivial partitions of this 10-mode state [26]. In parallel, by multiplexing pulse trains in the time domain, a continuous-variable cluster state containing more than 104 sequentially-entangled temporal modes was demonstrated, although its accessibility was limited to only two states at a time [22]. Using an intrinsically multimode quantum comb and a homodyne detection apparatus, both on-demand reconfigurable multimode entanglement and the simultaneous generation of 13 cluster states have been reported [23]. So far, all of the demonstrated cluster states have been scalable in one degree of freedom - either in frequency or in time. By entangling the quantum frequency comb in both the time and frequency continuous variables, it has been shown that a hybrid time-frequency square lattice cluster state suitable for universal quantum computing can be produced [36].

Besides using a resonant cavity to shape the energy spectrum of the entangled photons, a quantum frequency comb can also be created via spectral filtering after the generation process, as demonstrated using correlated frequency bins in $\chi^{(2)}$ PPLN with a narrowband fiber-based Bragg

grating filter [18], followed up by experiments based on programmable optical filters [37]. This spectral filtering method has been extended to create high-dimensional entanglement, including the verification of quDits (D=4) in PPKTP using spatial light modulators [19], the theoretical prediction of quDits with a dimensionality of several tens in AlGaAs Bragg reflection waveguides [38], and a demonstration of polarization-frequency hyper-entanglement in PPKTP using an external optical cavity filter [39]. Although this method has often been used to remove noise and define spectral properties, the spectral purity of the filtered photons is intrinsically reduced due to the fundamental trade-off between purity and heralding efficiency [40]. In addition, since any additional optical element is a source of losses, these applied filters not only reduce the number of available photon pairs, but also degrade the heralding efficiency of the device. To solve this issue, a technique called spectrally-resolved Hong-Ou-Mandel interference has been developed to successfully create frequency entangled quDits with $D > 10$ without the use of any spectral filters or resonant cavities [20].

Although large complex quantum states have been widely investigated, bulk optics based approaches and spectral-filtering methods require large, expensive, and very complex setups, not suitable for real-world applications outside of the lab. Another challenge for these systems is that when the OPO is pumped by a pulsed laser, active stabilization is required to ensure that the incident laser spectrum is perfectly aligned with the cavity resonances in most experiments [35, 36] (see Fig. 2(b)). Furthermore, the quantum states that have been demonstrated with this OPO approach have not yet achieved the level of squeezing required (with a threshold value of 20.5 dB) for fault-tolerant optical quantum computation [41], being typically limited by loss which degrades the squeezed states. In addition, the spectral modes of a large OPO cannot be individually addressed due to their small spectral separation. Reducing the size of the resonant cavities would allow access to individual frequency modes and, in turn, also allow one to exploit single or entangled photons instead of (or in addition to) squeezed states. Therefore, a platform made of highly nonlinear media in a small footprint is highly desirable for the generation of large-scale quantum states.

INTEGRATED QUANTUM FREQUENCY COMBS

In recent years, integrated (on-chip) photonics has stood out as a promising platform for quantum optics [42]. Compact and mass-producible photonic chips – particularly those compatible with the silicon chip industry – will enable compact, cost-efficient, and stable devices for the generation and processing of non-classical optical states. This is highlighted by demonstrations of on-chip photon sources, path-entangled quantum states, and basic algorithms [1, 2]. However, on-chip sources of quantum states and quantum gates have mainly focused on the use of polarization- or path-entangled photons, where the dimension of each state corresponds to a waveguide mode. These architectures are intrinsically limited, since the state/gate complexity directly scales with the quantum circuit footprint and complexity.

The on-chip generation of classical frequency combs is a very active research field, and many of its principles are reflected in the first demonstrations of on-chip quantum combs [5]. As materials used for on-chip integration typically exhibit third-order optical nonlinearity, spontaneous four-wave mixing (SFWM) is used for the generation of on-chip quantum frequency combs. In SFWM, the nonlinearity mediates the annihilation of two photons from an excitation field and the simultaneous generation of two daughter photons named signal and idler. Since the process occurs randomly, and the required pump power is typically very low (on the order of 10's of milliwatts, so that the probability of a pair event is at most only a few percent per pump

pulse), such photon pairs show strong correlations in time and frequency. To increase the efficiency of this process and also provide the equidistant-line feature of combs, cavity enhancement in on-chip resonant structures is used, particularly in high-quality factor microring resonators (Fig. 3) [43]. Due to the enhancement and self-filtering of the resonances, the generated photons exhibit high purity and brightness, and low noise backgrounds, properties that are desirable for quantum experiments.

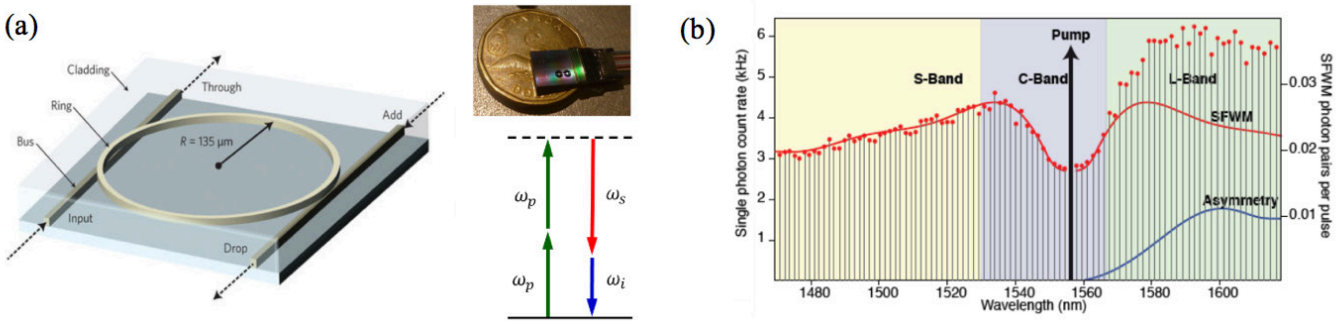


Fig.3. Quantum frequency comb generation in integrated Hydex resonators. (a) Via spontaneous four-wave mixing inside the nonlinear microcavity [43], two pump photons at frequency (ω_p) are converted to one signal and one idler photon at frequencies (ω_i and ω_s), with energy conservation demanding ($\omega_i+\omega_s=2\omega_p$). Inset: an integrated Hydex photonic chip compared to a Canadian one-dollar coin. (b) A broad measured quantum frequency comb spectrum spanning from the S to the L telecommunications band [11].

Such an integrated quantum frequency comb is important for quantum information processing because of its effective photon generation process [44, 45]. By optically exciting a single cavity resonance, SFWM symmetrically populates neighboring resonances with photon pairs, creating a highly stable source of several channels of heralded single photons (where the measurement of the signal heralds the presence of the idler, and vice versa) [5]. Using photon auto-correlation measurements, it was verified that a pure single frequency mode photon was generated in the signal and idler resonances, respectively, and that the bi-photon state has a Schmidt mode number of close to 1 (corresponding to a pure separable state) [21]. Selecting one pair of signal and idler photon resonances has enabled heralded sources in Si-microrings [4, 6] and Si-microdisks [7], as well as amorphous Si-microrings [9]. Entangled photon pair generation has been demonstrated in Si-microring resonators including time-bin [10, 13], energy-time [14-16], polarization [16], and time-bin entanglement in SiN [12] resonators.

Path-entanglement in silicon resonators has been demonstrated using two individual cavities [17]. In addition, because of the multi-channel property, these on-chip entangled quantum sources exhibit compatibility with telecommunications wavelength multiplexing techniques [5, 13, 15]. One challenge to all of these approaches, however, is that these schemes require external lasers in order to excite the cavities. This can be resolved through the use of an actively-modulated, nested-cavity configuration, which additionally enables the easy increase of the repetition rate of the excitation pulse train via harmonic mode-locking, and thus the increase of the pair production rates, while maintaining a low noise background and high photon purity [46].

The application of quantum frequency combs has evolved into the generation of large-scale quantum states, which can be achieved by increasing the number of entangled photons and/or their dimensionality. Although multi-photon entanglement [22, 23-26] and high-dimensional states [19, 20] have been demonstrated using

large-scale free-space optics, this has only been achieved in an integrated platform very recently. A double-pulse excitation of a single resonance was used to demonstrate the generation of time-bin entangled photon pairs over the entire frequency comb spectrum [11]. The distinctive multimode characteristic of the frequency comb allowed the demonstration of four-photon time-bin entangled photon states by post-selecting two signal and idler pairs on different resonances simultaneously. The realization of this four-photon entangled state was confirmed through quantum interference as well as quantum state tomography [11]. From a different point of view, photon pairs (signal and idler) can be generated in a quantum superposition of many frequency modes. This approach leads to the realization of two-photon frequency-entangled quDits, and resulted in the demonstration of a quantum system with at least one hundred dimensions, formed by two entangled quDits with D = 10 [21]. In order to perform deterministic quDit gate operations, a coherent manipulation platform with which to control frequency-entangled states was introduced using off-the-shelf telecommunications components (e.g. electro-optic phase modulators and programmable optical filters). The platform was validated by measuring Bell inequality violations and performing quantum state tomography for D=4. Frequency-bin qubits with 40 mode pairs were also investigated using SiN resonators with a FSR of 50 GHz [47].

Besides using a single resonator, quantum frequency combs have also been generated in coupled-resonator optical waveguides (CROWs) consisting of cascaded cavities [48, 49]. Due to the slow-light enhancement effort in the CROW device, where the group velocity of light slows down as a result of the spatial and temporal compression of the local energy density [50], the total number of generated photons in each passband scales quadratically with the resonator number N [51]. Although the bandwidth of each passband increases with the number of resonators, the CROW structure still provides a significant enhancement of pair generation at each frequency (e.g. in time-bin entanglement [48]) compared to that in straight waveguides. Furthermore, it has been shown that when one carefully tunes the resonances in the individual devices, each passband forms a quantum frequency comb since the N resonators create "supermodes" of its N transmission resonances within each passband [49]. Thus this structure has the potential of creating a double-level quantum frequency comb, where a narrowband frequency comb (with a number of resonances scaling with N) in each passband is buried inside a broadband quantum frequency comb, which is separated by the resonator FSR.

SUMMARY AND OUTLOOK

Optical quantum frequency combs are of high interest for quantum information processing. Due to their intrinsic multimode property, both in bulk setups and integrated chips, they are a scalable platform for generating qubits and even large-scale quantum states. Their versatility has been demonstrated by their use as single-photon, entangled-photon, high-dimensional, and multi-photon quantum state sources. The frequency domain provides a unique framework for the manipulation of quantum states in a single spatial mode using standard telecommunications components. Quantum information processing with frequency-encoded photons not only offers great potential towards building robust optical interconnects, but also brings the ubiquitous technology of well-established fiber optics to quantum photonics [28]. Their applications, as predicated in the realization of spectral linear quantum computing and the implementation of boson sampling, suggest they will keep playing an important role in future practical implementations of quantum technologies.

Manipulating a large number of frequency modes is still very challenging. Although $\chi^{(2)}$-based OPO's

can generate thousands of modes (with a FSR of hundreds of MHz), this process requires the additional stabilization and manipulation of individual modes - not possible with current technology. While on-chip $\chi^{(3)}$-based resonators allow stable and scalable photon generation, as well as coherent state control of each mode, due to the relatively large micro-cavity FSR (on the order of tens of GHz), only 10 frequency modes have been demonstrated in the integrated platform with the manipulation of up to 4 modes. Reducing the FSR by increasing the resonator circumference would, in principle, increase the number of accessible modes; however, the new FSR should still be large enough (>10 GHz - the resolution of state-of-art optical filters) for photonic components to address each mode individually. In addition, the photons would experience higher propagation loss inside the resonators because of the large cavity circumference. Further increasing the scale of quantum states by using multiple particles and/or combining several degrees of freedom is an option, as predicted with frequency combs generated by both bulk optics [26, 37] and on-chip [39, 52] approaches.

A new direction towards generating quantum frequency combs is to use $\chi^{(2)}$-based micro-cavities. This approach, which combines the advantages of high efficiency $\chi^{(2)}$ processes with on-chip stability and enhancement, has been used to generate entangled photons in LiNbO3 microdisks [53] and heralded photons in Al-Ni microring resonators [54], as well as being the basis of theoretical predictions focusing on photon pair generation in AlGaAs nanodisks [55]. Most importantly, this scheme has the potential to create enough squeezing to reach the fault tolerance threshold in quantum computing with continuous-variable cluster states [56]. In addition, since the pump is separated spectrally far from the generated photon pairs, resonators using $\chi^{(2)}$ spontaneous parametric down-conversion provide efficient pump suppression compared to cavity resonators based on $\chi^{(3)}$spontaneous FWM processes [54]. Moreover, since this platform also permits integrated low-loss, high-speed electro-optic phase modulation, it is promising for realizing sufficient on-chip filtering and monolithic integration in terms of generating and processing components.

The control and detection of quantum frequency combs is not yet fully integrated. High-isolation filters are indeed needed to separate the excitation field from the photons and the detectors, while the phase modulators processing these sources, in particular, require discrete bulk devices until comparable integrated components are developed [56]. Different platforms are suited to complementary functionalities. For example, $\chi^{(2)}$ materials permit integrated low-loss, high-speed electro-optic phase modulation, while $\chi^{(3)}$ materials allow integrated generation and efficient detection of quantum light. Therefore, hybrid systems, where the device material and geometry can be individually optimized, might be an alternative option for multi-functional integrated circuits, rather than the use of fully monolithic platforms.

In closing, though there is still a long way before we can apply optical quantum frequency combs in practical quantum computing, we believe that this approach may help address the increasing scalability demands of quantum technologies in the near future.

REFERENCES

[1] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," Nature, vol. 464, pp.45-53, 2010.

[2] J. L. O'Brien, "Optical quantum computing," Science, vol. 318, pp.1567-1570, 2007.

[3] T. Udem, R. Holzwarth, T. W. and Hänsch, "Optical frequency metrology," Nature, vol. 416, pp.233-237, 2002.

[4] N. C. Harris, D. Grassani, A. Simbula, M. Pant, M. Galli, T. Baehr-Jones, M. Hochberg, D. Englund, D. Bajoni, and C. Galland, "Integrated source of spectrally filtered correlated photons for large-scale quantum photonic systems," Phys. Rev. X, vol.4, 041047, 2014.

[5] C. Reimer, L. Caspani, M. Clerici, M. Ferrera, M. Kues, M. Peccianti, A. Pasquazi, L. Razzari, B. E. Little, S. T. Chu, D. J. Moss and R. Morandotti, "Integrated frequency comb source of heralded single photons," Opt. Express, vol. 22 pp. 6535-6546, 2014.

[6] S. Azzini, D. Grassani, M. J. Strain, M. Sorel, L. G. Helt, J. E. Sipe, M. Liscidini, M. Galli, and D. Bajoni, "Ultra-low power generation of twin photons in a compact silicon ring resonator," Opt. Express, vol. 20, pp. 23100-23107, 2012.

[7] W. Jiang, X. Lu, J. Zhang, O. Painter, and Q. Lin, "Silicon-chip source of bright photon pairs," Opt. Express, vol. 23, pp.20884-20904, 2015.

[8] C. Reimer, M. Kues, L. Caspani, B. Wetzel, P. Roztocki, M. Clerici, Y. Jestin, M. Ferrera, M. Peccianti, A. Pasquazi, B. E. Little, S. T. Chu, D. J. Moss and R. Morandotti, "Cross-polarized photon-pair generation and bi-chromatically pumped optical parametric oscillation on a chip," Nat. Commun., vol.6, 8236, 2015.

[9] E. Hemsley, D. Bonneau, J. Pelc, R. Beausoleil, J. L. O'Brien, and M. G. Thompson. "Photon pair generation in hydrogenated amorphous silicon microring resonators," Sci. Rep., vol. 6, 38908, 2016.

[10] R. Wakabayashi, M. Fujiwara, K. I. Yoshino, Y. Nambu, M. Sasaki, and T. Aoki, "Time-bin entangled photon pair generation from Si micro-ring resonator," Opt. Express, vol. 23, pp.1103-1113, 2015.

[11] C. Reimer, M. Kues, P. Roztocki, B. Wetzel, F. Grazioso, B. E. Little, S. T. Chu, T. Johnston, Y. Bromberg, L. Caspani, D. J. Moss, and R. Morandotti, "Generation of multiphoton entangled quantum states by means of integrated frequency combs," Science, vol. 351, pp.1176-1180, 2016.

[12] S. Ramelow, A. Farsi, S. Clemmen, A. Gaeta, D. Orquiza, K. Luke, and M. Lipson, "Silicon-nitride integrated source of narrowband entangled photon-pairs," Joint Annual Meeting of the Austrian Physical Society and the Swiss Physical Society together with the Austrian and Swiss Societies for Astronomy and Astrophysics, pp. 116, 2015.

[13] M. Fujiwara, W. Ryota, S. Masahide, and T. Masahiro, "Wavelength division multiplexed and double-port pumped time-bin entangled photon pair generation using Si ring resonator," Opt. Express, vol. 25, pp. 3445-3453, 2017.

[14] D. Grassani, S. Azzini, M. Liscidini, M. Galli, M. J. Strain, M. Sorel, J. E. Sipe, and D. Bajoni, "Micrometer-scale integrated silicon source of time-energy entangled photons," Optica, vol.2, pp. 88-94, 2015.

[15] F. Mazeas, M. Traetta, M. Bentivegna, F. Kaiser, D. Aktas, W. Zhang, C. Ramos, L. Ngah, T. Lunghi, E. Picholle, and N. B. Plougonven, "High-quality photonic entanglement for wavelength-multiplexed quantum communication based on a silicon chip," Opt. Express, vol. 24, pp.28731-28738, 2016.

[16] J. Suo, S. Dong, W. Zhang, Y. Huang, and J. Peng, "Generation of hyper-entanglement on polarization and energy-time based on a silicon micro-ring cavity," Opt. Express, vol. 23, pp.3985-3995, 2015.

[17] J. W. Silverstone, R. Santagati, D. Bonneau, M. J. Strain, M. Sorel, J. L. O'Brien, and M. G. Thompson, "Qubit entanglement between ring-resonator photon-pair sources on a silicon chip," Nat. Commun., vol.6, 7948, 2015.

[18] L. Olislager, J. Cussey, A. T. Nguyen, P. Emplit, S. Massar, J.-M. Merolla, and K. P. Huy, "Frequency-bin entangled photons," Phys. Rev. A, vol. 82, 013804, 2010.

[19] C. Bernhard, B. Bessire, T. Feurer, and A. Stefanov, "Shaping frequency-entangled qudits," Phys. Rev. A, vol. 88, 032322, 2013.

[20] R. B. Jin, R. Shimizu, M. Fujiwara, M. Takeoka, R. Wakabayashi, T. Yamashita, S. Miki, H. Terai, T. Gerrits, and M. Sasaki, "Simple method of generating and distributing frequency-entangled qudits," Quantum Sci. Technol., vol.1, 015004, 2016.

[21] M. Kues, C. Reimer, P. Roztocki, L. Cortes, S. Sciara, B. Wetzel, Y. Zhang, A. Cinio, S. T. Chu, B. E. Little, D. J. Moss, L. Caspani, J. Azana, and R. Morandotti, "On-chip generation of high-dimensional entangled quantum states and their coherent controls," Nature, vol. 546, pp. 622-626, 2017.

[22] S. Yokoyama, R. Ukai, S. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, "Ultra-large-scale continuous-variable cluster states multiplexed in the time domain," Nat. Photon. vol.7, pp. 982-986, 2013.

[23] Y. Cai, J. Roslund, G. Ferrini, F. Arzani, X. Xu, C. Fabre, N. Treps, "Multimode entanglement in reconfigurable graph states using optical frequency combs," Nat. Commun., vol. 8, 15645, 2017.

[24] M. Pysher, Y. Miwa, R. Shahrokhshahi, R. Bloomer, and O. Pfister, "Parallel generation of quadripartite cluster entanglement in the optical frequency comb," Phys. Rev. Lett., vol. 107, 030505, 2011.

[25] M. Chen, N. C. Menicucci, and O. Pfister, "Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb," Phys. Rev. Lett., vol. 112,120505, 2014.

[26] S. Gerke, J. Sperling, W. Vogel, Y. Cai, J. Roslund, N. Treps, and C. Fabre, "Full multipartite entanglement of frequency-comb Gaussian states," Phys. Rev. Lett., vol.114, 050501, 2015.

[27] C. Joshi, A. Farsi, and A. Gaeta, "Frequency-domain boson sampling," Conference on Lasers and Electro-Optics, pp. FTu1F.1, 2017.

[28] J. M. Lukens, and P. Lougovski, "Frequency-encoded photonic qubits for scalable quantum information processing," Optica, vol. 4, pp.8-16, 2017.

[29] D. Arslanov, M. Spunei, J. Mandon, S. Cristescu, S. Persijn, and F. Harren, "Continuous-wave optical parametric oscillator based infrared spectroscopy for sensitive molecular gas sensing," Laser Photonics Rev., vol. 7, pp.188-206, 2013.

[30] J. Roslund, R. Arajo, S. Jiang, C. Fabre, and N. Treps, "Wavelength-multiplexed quantum networks with ultrafast frequency combs," Nat. Photon., vol.8, pp.109-112, 2014.

[31] J. Zhang and S. L. Braunstein, "Continuous-variable Gaussian analog of cluster states," Phys. Rev. A, vol. 73, 032318, 2006.

[32] N. C. Menicucci, P. Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, "Universal quantum computation with continuous-variable cluster states," Phys. Rev. Lett., vol. 97, 110501, 2016.

[33] L. Wu, H. Kimble, J. Hall, and H. Wu, "Generation of squeezed states by parametric down conversion", Phys. Rev. Lett., vol. 57, 2520, 1986.

[34] M. Wolinsky and H. Carmichael, "Quantum noise in the parametric oscillator: from squeezed states to coherent-state superpositions," Phys. Rev. Lett., vol. 60, 1836, 1988.

[35] O. Pinel, P. Jian, R. Araujo, J. Feng, and B. Chalopin, "Generation and characterization of multimode quantum frequency combs," Phys. Rev. Lett., vol.108, 083601, 2012.

[36] R. N. Alexander, P. Wang, N. Sridhar, M. Chen, O. Pfister, N. C. Menicucci, "One-way quantum computing with arbitrarily large time-frequency continuous-variable cluster states from a single optical parametric oscillator," Phys. Rev. A, vol. 94, 032327, 2016.

[37] J. M. Lukens, O. Odele, C. Langrock, M. M. Fejer, D. E. Leaird, and A. M. Weiner, "Generation of biphoton correlation trains through spectral filtering," Opt. Express, vol. 22, pp. 9585-9596, 2014.

[38] C. Autebert, A. Minneci, G. Maltese, A. Lemaître, M. Amanti, T. Coudreau, P. Milman, and S. Ducci, "On-chip generation of frequency-entangled qudits," Quantum Information and Measurement, pp. QW2C-2, 2017.

[39] Z. Xie, T. Zhong, S. Shrestha, X. Xu, J. Liang, Y. Gong, J. Bienfang, A. Restelli, J. H. Shapiro, F. N. C. Wong, and C. W. Wong, "Harnessing high-dimensional hyperentanglement through a biphoton frequency comb," Nat. Photonics, vol.9, pp.536–542, 2015.

[40] E. M. Scott, N. Montaut, J. Tiedau, L. Sansoni, H. Herrmann, T. J. Bartley, and C. Silberhorn, "Limits on the heralding efficiencies and spectral purities of spectrally filtered single photons from photon-pair sources," Phys. Rev. A, vol. 95, 061803, 2017.

[41] N. C. Menicucci, "Fault-tolerant measurement-based quantum computing with continuous-variable cluster states," Phys. Rev. Lett., vol.112, 120504, 2014.

[42] D. Bonneau, J. Silverstone, and M. Thompson, "Silicon quantum photonics, in silicon photonics III," edited by Pavesi L. and D. J. Lockwood (Springer International Publishing AG), pp. 41–82, 2016.

[43] D. J. Moss, R. Morandotti, A. L. Gaeta, and M. Lipson, "New CMOS-compatible platforms based on silicon nitride and Hydex for nonlinear optics," Nat. Photon., vol. 7, pp. 597-607, 2013.

[44] A. Pasquazi, M. Peccianti, L. Razzari, D. J. Moss, S. Coen, M. Erkintalo, Y. K. Chembo, T. Hansson, S. Wabnitz, P. Del'Haye, X. Xue, A. M. Weiner, R. Morandotti, "Micro-combs: A novel generation of optical sources," Phys. Rep., 2017.

[45] L. Caspani, C. Reimer, M. Kues, P. Roztocki, M. Clerici, B. Wetzel, Y. Jestin, M. Ferrera, M. Peccianti, A. Pasquazi, L. Razzari, B. E. Little, S. T. Chu, D. J. Moss, and R. Morandotti, "Multifrequency sources of quantum correlated photon pairs on-chip: a path toward integrated quantum frequency combs," Nanophotonics, vol. 5, pp. 351-362, 2016.

[46] P. Roztocki, M. Kues, C. Reimer, B. Wetzel, S. Sciara, Y. Zhang, A. Cinio, B. E. Little, S. T. Chu, D. J. Moss, and R. Morandotti, "Practical system for the generation of pulsed quantum frequency combs," Opt. Express, vol.25, pp.18940-18949, 2017.

[47] P. Imany, J. Villegas, O. Odele, K. Han, D. Leaird, M. Qi, D. E. Leaird, and A. Weiner, "Demonstration of frequency-bin entanglement in an integrated optical microresonator," Conference on Lasers and Electro-Optics, pp. JTh5B.3, 2017.

[48] H. Takesue, N. Matsuda, E. Kuramochi, and M. Notomi, "Entangled photons from on-chip slow light," Sci. Rep., vol.4, 3913,2014.

[49] R. Kumar, J. R. Ong, M. Savanier, S. Mookherjea, "Controlling the spectrum of photons generated on a silicon nanophotonic chip," Nat. Commun., vol. 5, 5489, 2014.

[50] A. Melloni, F. Morichetti, and M. Martinelli, "Four-wave mixing and wavelength conversion in coupled-resonator optical waveguides," J. Opt. Soc. Am. B, vol. 25, pp.C87-97, 2008.

[51] L. G. Helt, J. E. Sipe, and Marco Liscidini, "Super spontaneous four-wave mixing in single-channel side-coupled integrated spaced sequence of resonator structures," Opt. Lett., vol. 37, pp. 4431-4433, 2012.

[52] Y. Wen, X. Wu, R. Li, Q. Lin, and G. He, "Five-partite entanglement generation in a high-Q microresonator," Phys. Rev. A, vol. 91, pp. 042311, 2015.

[53] I. Frank, J. Moore, J. Douglas, R. Camacho, and M. Eichenfield, "Entangled photon generation in lithium niobate microdisk resonators through spontaneous parametric down conversion," Conference on Lasers and Electro-Optics, pp. STh3P.1, 2016.

[54] X. Guo, C. L. Zou, C. Schuck, H. Jung, R. Cheng, and H. X. Tang, "Parametric down-conversion photon-pair source on a nanophotonic chip," Light Sci. Appl., vol. 6, e16249, 2017.

[55] G. Marino, A. Solntsev, L. Xu, V. Gili, D. Smirnova, H. Chen, G. Zhang, A. Zayats, C. Angelis, G. Leo, and Y. Kivshar, "Sum-frequency generation and photon-pair creation in AlGaAs nano-scale resonators," Conference on Lasers and Electro-Optics, pp. FTu4D-2,2017.

[56] W. Pernice, C. Schuck, O. Minaeva, M. Li, G. Goltsman, V. Sergienko, and H. Tang, "High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits," Nat. Commun., vol.3, 1325, 2012.

AUTHOR BIOGRAPHIES

Yanbing Zhang is an early career researcher working in nonlinear optics, quantum photonics and fiber lasers.

Piotr Roztocki is pursuing his PhD at the INRS-EMT. He is interested in applied and fundamental research in the fields of nonlinear, integrated, and quantum optics.

Christian Reimer is an early career physicist working on integrated nonlinear optics with a focus on the generation of entangled quantum states, as well as classical and quantum optical frequency combs and mode-locked lasers.

Stefania Sciara is a PhD student at INRS-EMT. Her research focuses on the theoretical investigation of complex optical entangled quantum states, finalized to their experimental implementation.

Dr. Michael Kues is an early career physicist specialized in optics. His research focuses on exploring new physical concepts in integrated photonics systems for optical quantum information processing.

Professor David Moss is Director of the Center for Microphotonics at Swinburne University in Melbourne, Australia, leading research programs in a wide variety of areas including integrated nonlinear nanophotonics, telecommunications, quantum optics, biophotonics, renewable energy and others. He received a B.Sc. in physics from the University of Waterloo, Canada, and a Ph.D. in nonlinear optics from the University of Toronto, Canada, in 1988. From 1988-92, he was with the National Research Council of Canada at the Institute for Microstructural Sciences in Ottawa working on III–V optoelectronic devices. From 1992-4 he was a Senior Visiting Scientist at the Hitachi Central Research Laboratories, Tokyo, Japan, working on high-speed optoelectronic devices. From 1994-8, he was a Senior Research Fellow at the Optical Fiber Technology Center, University of Sydney, Australia. From 98 to 2003 he was a Manager at JDS Uniphase, Ottawa, Canada, leading a team developing products for 40Gb/s telecommunications systems. From 2003-13 he was with the University of Sydney and the Centre for Ultra-high Bandwidth Devices for Optical Systems (CUDOS) working on ultrahigh bandwidth optical signal processing nonlinear nanophotonic devices. He has about 600 journal and conference papers including a Nature, Science, 6 Nature Photonics and 4 Nature Communications papers. He won the 2011 Australian Museum Eureka Science Prize and Google Australia Award for innovation in computer science. He has been active on many conference committees, including General Chair of OSA Integrated Photonics Research (IPR) in in New Orleans (2017). He is a Fellow of the IEEE Photonics Society and Fellow of the Optical Society of America.

Roberto Morandotti, professor at INRS-EMT since 2008, has broad experience in the field of photonics, ranging from the fabrication of integrated devices to the use of state-of-the-art optical characterization techniques. He pioneered the realization of integrated classical and quantum frequency combs. He is a Fellow of the Royal Society of Canada, of the American Physical Society, of the Optical Society of America, of the SPIE and of the Institute of Physics (UK), among others.

Quantum Cryptography and Side Channel Attacks

by: Colin Lualdi, Stephen Pappas, Daniel Stack, and Brandon Rodenburg

Quantum Information Science Group, The MITRE Corporation

ABSTRACT

Quantum key distribution (QKD) promises a theoretically unbreakable cryptosystem by employing the probabilistic nature of quantum measurement over mutually unbiased bases, making it superior to classical cryptosystems threatened by the advent of quatnum computing. However, it has been shown that QKD systems are vulnerable to side channel attacks due to engineering and technical imperfections in practical implementations. This article presents a general overview of quantum cryptography, beginning with a comparison of classical and quantum cryptography is threatened by quantum computing. A basic discussion of QKD's security characteristics and implementation details is given. An example side channel attack is introduced with the avalanche photodiode backflash attack. The authors provide a brief overview of their experiment to investigate this attack, and report results indicating the ability for this attack to, in principle, succeed.

1 INTRODUCTION

Quantum key distribution (QKD) promises a theoretically unbreakable cryptosystem by employing the probabilistic nature of quantum measurement over mutually unbiased bases. Its security lies in the impossibility of an eavesdropper to gain access to the quantum keys without revealing their presence due to the destructive nature of quantum measurement, as measured by the quantum bit error rate (QBER) [1]. However, it has been shown that QKD systems possess security vulnerabilities due to engineering and technical imperfections in practical implementations. Side channel attacks exploiting various points of accidental information leakage have been described in the literature, with examples including the photon number splitting and faked states attacks [1, 2, 3].

Many of those systems employ avalanche photodiodes (APDs) as a part of the process of measuring photon states to create a secure key as described by QKD protocols like BB84 [1]. Avalanches of charge carriers following photodetection events in silicon and InGaAs APDs are known to emit secondary photons as a consequence of carrier relaxation [4, 5]. These photons, or backflashes, may be coupled back into the quantum channel and detected by an eavesdropper who could potentially deduce the states of the original information-carrying photons measured by the legitimate QKD receiver without affecting the QBER and thus remain hidden [6, 7].

2 QUANTUM CRYPTOGRAPHY

2.1 The One-Time Pad

Many encryption systems varying in complexity and security have been invented. However, in the context of quantum cryptography the one-time pad plays an important role. The principle behind this cryptosystem (also known as the Vernam cipher) is simple, yet it is extremely effective at securing information [9]. Suppose we have a system where we assign a numerical value to each letter in the alphabet:

Letter	A	B	C	...	Y	Z
Number	1	2	3	...	25	26

We can use this to obtain numerical equivalents of ordinary text. For instance C A T would translate to 3 1 20. Suppose a person, Alice, wishes to send her friend, Bob, the message C A T but she does not want anyone to intercept her message and read its contents. So she and Bob agree to use a one-

time pad to encrypt the message. Prior to sending the message, Alice and Bob meet in person and generates a string of three random numbers: 4 13 6. They both record those numbers, keeping them secret, and go their separate ways.

When Alice is ready to send her message, she first converts her message, C A T, to its numerical equivalent, 3 1 20. She then adds her three random numbers (the key) to her numerical message, one by one:

	3	1	20
+	4	13	6
	7	14	26

Alice obtains 7 14 26 as a result, and sends this to Bob over an unsecured channel (e.g. email). Note that translating this sequence of numbers to letters would yield a meaningless G N Z. Upon receiving the message, Bob simply subtracts the random numbers selected earlier:

	7	14	26
+	4	13	6
	3	1	20

Translating those numbers to letters, Bob obtains the original message, C A T.

This is the general procedure of the one-time pad. Its security lies in the fact that random numbers were used to encrypt the message prior to transmission. Because of this, it is impossible for an eavesdropper, Eve, who manages to intercept this message midtransmission, to decipher it. All Eve knows is G N Z (7 14 26). She has no additional information regarding the encryption key used, so while she could guess, she cannot find the correct decryption with certainty [9]. For example, she would not be able to confidently identify the correct message if she gets either C A T or B O B as a result of her decryption attempt.

In his 1949 paper, C.K. Shannon proves that as long as the random key is only used once and is the same length as the message itself (or longer), the one-time pad is capable of achieving perfect secrecy [10]. The random nature of the one-time pad transformation does not skew the probability distribution of possible encrypted messages such that an eavesdropper would be able to deduce the original message through probabilistic analysis of the encrypted message [9].

This naturally leads us to recognize the main limitations of the one-time pad. First, one-time pad keys can be used only once. Otherwise, if the same key was used multiple times, Eve would be able to use facts such as that certain words occur more frequently than others in English to improve her chances of guessing the key [9]. Second, for reasons similar to the one-time-use requirement, the length of the keys used must be longer than the actual message itself.

Those limitations are the main factors preventing the widespread adoption of the onetime pad as an encryption standard. There is no known classical means of distributing (or regenerating) a key with absolute security. Additionally, for frequent and lengthy communications, extremely large amounts of keys would be required. Even worse, carrying around a packet of all the pre-made keys makes them susceptible to theft. Finally, the logistics of coordinating all the keys become prohibitively difficult when scaling up from two people (Alice and Bob) to large institutions.

2.2 Public Key Cryptography

Due to the inherent difficulties of the one-time pad, the majority of modern-day encryption schemes rely on public key cryptography, which works differently from the one-time pad. Generally, with a public key cryptosystem, the receiver (Bob) performs a procedure to create two keys that share a mathematical relationship, one public and one private. Bob then announces the public key while keeping the private key a secret.

Upon receiving the public key, the sender (Alice) can then use it to encrypt a message such that the

encryption process is a "one-way function" [11]. That is, the public key cannot decrypt the encrypted message. Alice then sends the encrypted message to Bob, who can decrypt it with his private key due to the mathematical relationship between the public and private keys. Intuitively, this is similar to "encrypting" a message by putting it in a USPS mailbox. Nobody except the postal worker has the "private" key to the mailbox, so he is the only person who can decrypt the letter by unlocking the mailbox.

A common public key cryptosystem is RSA, introduced in 1978 [11]. RSA relies critically on the difficulty of factoring large numbers. To date, there is no known classical algorithm capable of factoring integers in polynomial time. The fastest, well-known classical factoring algorithms, such as the Number Field Sieve, run in time of order $\exp[(\log(N))^{1/3}(\log\log(N))^{2/3}]$, scaling exponentially in time [13]. As a result, Eve cannot factor the key fast enough to discover the secret message while it still has value to Alice and Bob. Assuming each each computer operation takes 1 µs, a 50 digit key would require roughly 4 hours, but a 200-digit key would require almost 4 billion years to factor [11].

Because public-key cryptosystems like RSA permit Alice and Bob to send encrypted messages without the need to agree on a secret key beforehand, those cryptosystems have proven to be much more practical to implement on a global scale than the one-time pad and secure the majority of our electronic communications today.

2.3 Impact of Quantum Computers on Classical Cryptography

The discovery of a practical polynomial-time factoring algorithm would suddenly cast the security of cryptosystems like RSA in doubt, with far-reaching effects on the foundations of our society. For this reason, Peter Shor caught the attention of the cryptography community in 1994 when he discovered an algorithm (now known as Shor's algorithm) capable of factoring in polynomial time [14] using a quantum computer.

The factoring problem is in fact a period-finding problem in disguise, which Shor's algorithm is able to solve much more efficiently than classical algorithms. While Shor's algorithm includes several procedures that may be performed efficiently on a classical computer, its core consists of the quantum Fourier transform (QFT). The classical fast Fourier transform (FFT) requires a computational time proportional to $n2^n$ (compared to $(2^n)2$ for the brute force solution), where n is the number of bits. In contrast, the quantum Fourier transform runs in time proportional to n^2, which is significantly faster [12]. The combined algorithm requires poly$(\log(N))$ steps for a general input N, which is polynomial time [13].

Fortunately, quantum computers did not exist in 1994 and Shor's algorithm remained a harmless theoretical exercise. However, since then there has been significant progress in the building of practical quantum computers and a replacement for public key cryptosystems is necessary.

3 QUANTUM KEY DISTRIBUTION

Fortunately, while the advent of quantum information (i.e. quantum computers) is the bane of the information security world, it also presents a possible solution in the form of quantum key distribution (QKD), which revisits the theoretically secure one-time pad. As its name implies, QKD attempts to address the main disadvantage of the one-time pad by solving the secure distribution problem with the probabilistic nature of quantum measurement [1].

QKD was first introduced in 1984 by Charles Bennett and Gilles Brassard [16]. In their paper, they describe a protocol, now known as BB84, to permit the secure distribution of keys. The sender encodes keys in quantum states such as photon polarization, and then transmits those states to a receiver, who measures them (e.g. determine photon polarization). Both parties then perform post-processing to obtain a secret key and to confirm that it has been transmitted securely.

Suppose we have two individuals who wish to establish secure communication, Alice and Bob. While Alice and Bob are physically separated, they are connected by a single optical fiber cable. They also have access to ordinary, unsecured classical communication channels (such as the Internet).

1. Alice creates randomly polarized photons and sends them to Bob

As the first step, Alice creates a long sequence of qubits in the form of randomly polarized photons. When modeled as a two-state quantum system, photon polarization consists of two quantum states that form a complete orthogonal basis spanning the two-dimensional Hilbert space. A common pair of basis states is horizontal *(|Hi = |0i)* and vertical *(|V i = |1i)*. Through superposition, two additional orthogonal states can be created (non-orthogonal to *H* and V): the diagonal *(|Di)* and antidiagonal *(|Ai)*. Those states are defined as:

$$|D\rangle \equiv \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle \quad (1)$$

$$|A\rangle \equiv \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-\rangle \quad (2)$$

So, prior to creating each photon qubit, Alice chooses a random polarization basis *(HV* or *AD)*. She records this information. Then, she creates the photon with a random polarization state within that basis. She also records this polarization state and its associated bit value. Note that upon measurement *|Hi* and *|Di* correspond to bit *0* and *|V i* and *|Ai* correspond to bit 1. Thus, each photon that Alice creates has a random polarization state with a 25% probability of being *|Hi, |V i, |Ai,* or |Di. She then transmits the qubit to Bob via their optical fiber cable.

2. Bob receives the qubits from Alice and measures them

Upon receiving the photons from Alice, Bob measures their polarization states to begin the process of creating a secret key. As follows from the basic principles of quantum mechanics, the basis that Bob uses for his measurements will affect their outcome. For each photon that Bob receives, he randomly chooses either the HV or AD basis, and performs the measurement. He records his basis choices and measurement results in the form of random bits.

3. Alice and Bob compare results

As the final step in the BB84 protocol, Alice and Bob indirectly compare their random bits to obtain a sifted key. Alice announces to Bob over an insecure classical channel her random basis choices while keeping secret her state choices. Bob looks at his basis choices, and tells Alice which photons had Alice and Bob choosing the same basis, and which had a basis mismatch. Bob communicates this information to Alice over the insecure classical channel, keeping secret his measurement outcomes. Alice and Bob then agree to keeping measurements when their measurement basis matched, and discarding all other measurements.

This step is significant because in keeping only the photons for which Bob knows he used the same basis as Alice, he can be certain that the random bit resulting from his measurement is exactly the same random bit that Alice obtained when randomly choosing a polarization state prior to photon transmission, due to the nature of quantum measurement. So the BB84 protocol allows Alice and Bob to create two sets of sifted keys of random bits that they know are identical just by comparing basis choices so that their actual random bits remain secret.

As a result, Alice and Bob now share a string of random bits that they can use as their secret key for the proved-secure one-time pad procedure as discussed earlier. Note that the one-time pad also works with strings of random bits [9, 12]. Suppose Alice uses an encoding system to convert her secret alphanumerical message to the binary string "10111001." The secret key that she shares with Bob might be "11001101." She performs bitwise modulo-2 sum (XOR) with her message and the

secret key to encrypt it:

	1	0	1	1	1	0	0	1
	1	1	0	0	1	1	0	1
⊕	0	1	1	1	0	1	0	0
	0	1	1	1	0	1	0	0
⊕	1	1	0	0	1	1	0	1
	1	0	1	1	1	0	0	1

Upon receiving the encrypted message from Alice, Bob can perform another bitwise modulo-2 sum using the shared secret key to decrypt the message:

There are additional error correction and privacy amplification protocols that Alice and Bob can perform to increase the secrecy and accuracy of their secret key, at the expense of reducing the number of bits in the key. The majority of those protocols are classical, and take place after the transmission of information through the quantum channel [1].

Key distribution via QKD has been proved theoretically secure against all attacks due to the probabilistic nature of quantum measurement. Any attempts by an eavesdropper to secretly measure the quantum bits mid-transmission will irrevocably alter those quantum states such that Alice and Bob will be aware that their quantum bits have been tampered with by measuring the QBER. Even with a quantum computer an eavesdropper cannot non-destructively measure or clone quantum states due to the quantum no-cloning theorem [17].

4 QKD IMPLEMENTATION

In addition to the well-known BB84 protocol, researchers have developed a number of alternative protocols. Some of them are variations of BB84, with differences in procedures and states used [1]. For instance, the E91 protocol, introduced by Arthur Ekert in 1991, involves creating entangled pairs of photons (Einstein-Podolsky-Rosen states) at a central source and sending each photon to Alice and Bob for measurement [19].

Due to the variety of available QKD protocols and two-state quantum systems, there are countless possible approaches to implementing QKD. Each has its own unique design corresponding to the requirements of the protocol and the use case, and comes with its own strengths and weaknesses in terms of QBER tolerance thresholds, key generation rate, feasibility, and other factors. For instance, while in the previous chapter we considered a general polarization-based implementation of BB84 using optical fibers, it is also possible to implement BB84 using photon phase and frequency encoding [1]. Additionally, one is not restricted to the use of optical fibers for qubit transmission; free-space QKD where photons are transmitted kilometers through the atmosphere along a shared line of sight have been demonstrated [20]. Commericial QKD systems are currently available for purchase, with many field tests conducted in recent years proving their feasibility [22, 23].

4.1 Exploiting Implementation Flaws

In the ideal QKD implementation, guaranteed security against eavesdroppers relies on the assumption that only idealized equipment is used where every component functions precisely as expected. However, real-world implementations tend to be far from ideal due to a variety of technical and engineering challenges. Such implementation flaws could significantly threaten the security of QKD as they offer side channel exploitation opportunities for Eve to increase her eavesdropping abilities without detection [1].

An example of a side channel attack is the backflash leakage attack, which exploits the physical implementation of a typical BB84 fiber-based system with polarization encoding . In such a system, the quantum state of photons transmitted by Alice is typically measured by Bob by routing the photons through a series of beamsplitters (non-polarizing and polarizing) and additional optics such that a photon in one of the four polarization states used

is ultimately detected by a photodetector (out of four total) that is associated with that polarization state. Hence, when Bob receives a signal from a photodetector associated with a certain polarization state, he knows that he has received a photon in that polarization state.

Figure 1 shows a typical BB84 receiver that achieves this measurement of the photon state. It consists of two arms, each with two single photon detectors. Each arm is associated with one of the two BB84 bases *(HV* or *AD)*, and is responsible for measuring photons in its basis. The 50-50 beamsplitter that connect the two arms performs the step of randomly choosing the basis for Bob by sending the incoming photons into either the HV or the AD arm with equal probabilities.

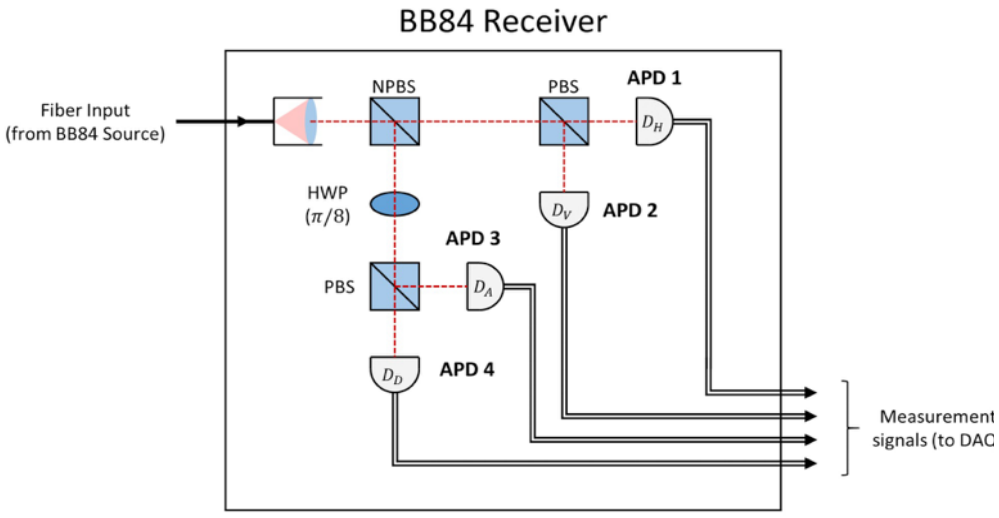


Figure 1: Schematic of a typical BB84 receiver layout. Figure credit: Stephen Pappas, MITRE & Colin Lualdi.

If the photon travels straight through the first beamsplitter, it enters the HV arm and Bob is measuring in this basis. The measurement process begins when the photon passes through a polarizing beamsplitter that directs the photon according to its polarization. For example, an H polarized photon continues straight through and is detected by an avalanche photodiode (APD), a common type of photodetector. Thus, when Bob sees this specific APD fire, he knows that he has chosen the HV basis, and the result of his measurement was H (which can be translated to a bit value). Similarly, a V polarized photon gets deflected by the polarizing beamsplitter and is directed into the second APD in the HV arm, registering as a V measurement.

On the other hand, if the photon is directed into the second measurement arm by the first beamsplitter, then Bob is measuring in the AD basis. As the beamsplitters measure in the HV basis, Bob needs to first rotate the polarization of the incoming AD photon by $\pi/4$ using a half-wave plate (HWP) so that a D photon becomes an H photon and an A photon becomes a V photon. The remainder of the measurement process is the same as in the HV arm except that when one of those APDs fire, Bob knows he is measuring in the AD basis and records an A measurement for one and a D for the other.

Those APDs have design flaw that could serve as a source of information leakage. First pointed out by Kurtsiefer et al., this attack relies on the curious fact that avalanche photodiodes are known to emit backflash photons upon photonic stimulation due to the physics of those detectors [6].

Their operating principle lies in the use of a semiconductor p-n junction. Prior to single photon detection, the reverse bias voltage of the p-n junction

[1] Most commercial fiber-based QKD systems actually employ alternative encoding schemes due to the susceptibility of the polarization states to disturbances from birefringence and other environmental effects that are difficult to manage outside of the laboratory setting [22].

is raised to a breakdown voltage V_b. At this voltage, absorption by even a single photon is sufficient to create carriers in the conduction band of the diode, which can then trigger an avalanche process, creating a measurable current in the milliamp range indicating photon detection. Different semiconductor materials are used for photons of different wavelengths. Silicon (Si) APDs are most sensitive to wavelengths in the 400-1000 nm range (ideal for laboratory experiments), while alternative semiconductor materials such as indium gallium arsenide are well suited for telecommunication wavelengths of 1300 nm or 1550 nm (ideal for long distance transmission).

When photons strike the semiconductor material, they cause electron excitations, creating electron-hole pairs. The electrons function as charge carriers (i.e. hot carriers or free carriers) and multiply, causing the avalanche. Interestingly, a photoemission also occurs as a result of those avalanches. Explanations for those photoemissions are varied and include radiative electron-hole recombination and carrier energy relaxation (direct, phonon-assisted, or Bremsstrahlung) [24, 25]. Those secondary photons may be either absorbed in a quiescent region of the semiconductor, initiating new avalanches, or they may find their way out of the detector [4].

Photons that manage to escape the detector could potentially be a source of information leakage when APDs are used in a QKD implementation. Such backflash photons could couple with the optical fiber leading into the APDs, find their way through Bob's QKD receiver, and out into the quantum channel traveling in the opposite direction of the incident photons from Alice. An eavesdropper could then discreetly siphon off the backflash photons, leaving the original photons untouched. If those backflash photons carry meaningful information corresponding to the information carried by the original photons, Eve could potentially perform measurements on her backflash photons to gain information about the results of Bob's measurements and, in extension, the secret key.

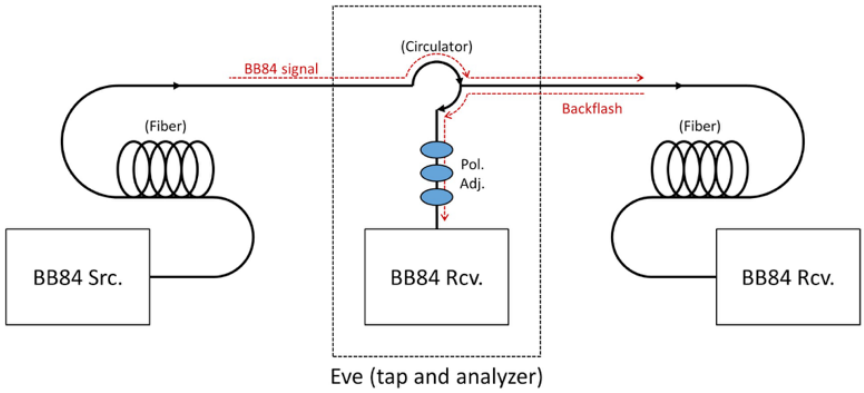


Figure 2: Overview of a potential QKD attack exploiting APD backflash emission.

Since the creation of backflash photons is a random process, Alice and Bob have no knowledge of or control over photons that escape Bob's receiver. Thus, this attack allows Eve to obtain copies of the photons used by Alice and Bob without their knowledge, and thus leave the QBER unaffected. Consequently, this represents a dangerous potential QKD vulnerability.

5 DEMONSTRATION OF INFORMATION LEAKAGE FROM APD BACK-FLASHES

We consider the hypothetical attack scenario shown in Figure 2. Alice and Bob are using a fiber-based BB84 QKD implementation with polarization encoding. It is assumed that Eve has full access to all classical communications between Alice and Bob. We also propose that Eve is able to tap into the quantum channel, perhaps with the use of an optical circulator. This would allow all the photons sent by Alice to Bob to travel uninterrupted, but diverts to Eve the backflash photons traveling in the opposite direction.

Due to the design of the BB84 receiver (see Figure 1), all backflash photons acquire specific polarization information as they exit their originating APD and travel through a sequence of polarizing beamsplitters and half-wave plates. For instance, APD1, being parallel to its polarizing beamsplitter, is responsible for measuring H-polarized photons. Therefore, when backflash photons exit APD1, they return through the polarizing beamsplitter where only H light is transmitted, and photons of different polarizations are reflected and lost.

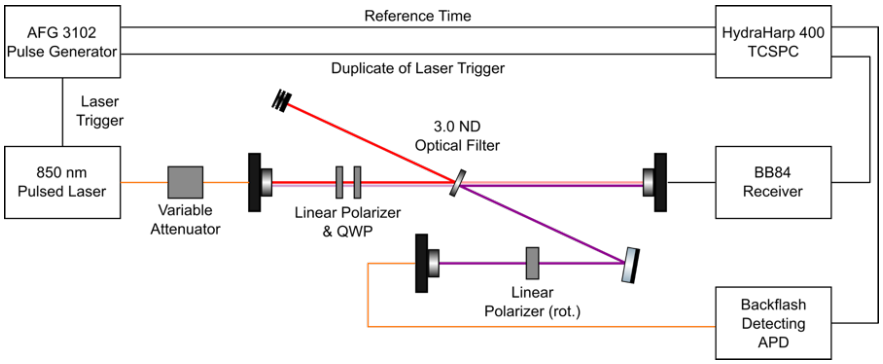


Figure 3: Schematic of the experiment setup used by the authors to investigate BB84 backflashes.

Those H photons then reach the main beamsplitter, where half of them are transmitted through to the quantum channel and the other half are lost. A similar process occurs with the remaining APDs: backflashes from APD2 reach the quantum channel as V photons and APDs 3 and 4 also produce D and A-polarized backflashes, respectively, as they exit the polarizing beamsplitter and half-wave plate set to 45 degrees.

It is important to emphasize that there is no direct coherence, classical or quantum, between the incident photons from Alice and the backflash photons. This is because the original photon is completely destroyed in the measurement process within the APDs. The resulting backflash creates a pulse of light that is created simply as a result of hot carrier relaxation. However, as those backflashes exit the BB84 receiver, the key polarization information is imprinted onto them by the various optical elements used. Additionally, a single QKD photon may create many backflash photons, allowing Eve to measure the polarization of the QKD signal with very high fidelity.

5.1 Experimental Apparatus

Figure 3 provides an overview of the experimental setup. A function generator acts as a pulse generator and serves as the timekeeper for the entire apparatus by setting the reference time. It triggers a 850 nm pulsed diode laser. A variable attenuator significantly reduces the laser's power so that it generates faint pulses in an approximation of a single photon source.

The resulting photons are then directed through through a linear polarizer set to 45 degrees with respect to the fast and slow axes of the immediately following quarter wave plate. This transforms the incoming photons into circular polarization. This is necessary in order to ensure the balanced distribution of all incoming photons among the four BB84 detectors as polarized beamsplitters evenly split circularly polarized light. The photons then pass through a neutral density (ND) filter with an optical density of 3.0 rotated ≈ 20 degrees off the beam axis and then routed to the BB84 receiver (see Figure 1 for details). Each BB84 measurement port contains a Si APD for photodetection. Some of the secondary photons resulting from the avalanches within those APDs manage to escape into the BB84 receiver, becoming backflash photons. A portion of those photons then exit the BB84 receiver (purple beam in Figure 3) and find their way back to the ND filter. The backflash photons reflect off the ND filter and coupled into a multimode optical fiber and detected by a silicon APD.

To permit the investigation of polarization correlations between individual backflash signals and detection

events in the 4-Channel APD (the originating APD of the backflash), we rotate a linear polarizer in front of the fiber capture to scan through the linear polarization Hilbert space. Each of the five output signals from the five APDs used is routed to a timetagger device that records the exact times of all individual photodetection events.

5.2 Experimental Results

Since we are interested in observing correlations between backflash polarization and individual APDs in the 4-Channel APD, during the data-processing step we isolate backflash events associated with a particular APD. We achieve this by identifying all photodetection times from the backflash detecting APD that occur within a specific time window after the firing of one of the four APDs in the BB84 receiver since that backflash photon must have originated from that BB84 APD. Note that this approach does not handle the case where additional backflash events from other APDs happen to occur whether because of a pulse with multiple photons or spontaneous emission within the same time window and therefore are incorrectly attributed to this APD. However, we make the reasonable assumption that such peculiar events are rare and their effects will be masked by legitimate backflashes that occur much more frequently.

Rotating the linear polarizer, we observe that the intensities of backflash events associated with each APD change as a function of the polarizer angle due to the hypothesized polarization dependence of the backflashes. Therefore, we are able to measure the maximum and minimum intensities of the backflashes from each APD.

We calculate the fringe visibility

$$\nu = \frac{I_{max} - I_{min}}{I_{max} + I_{min},} \tag{3}$$

where I_{max} is the maximum observed intensity and I_{min} is the minimum observed intensity. We apply this concept to our backflash measurements to give a quantitative measure of our ability to measure a specific polarization in the backflash data.

Figure 4 presents the visibility values for the five primary slices from each APD with $\nu = 0$ indicating minimum visibility and $\nu = 1$ indicating maximum visibility. With visibility values generally above 0.5, it is clear that we do have an ability to identify the polarization angles associated with maximum and minimum counts for each APD.

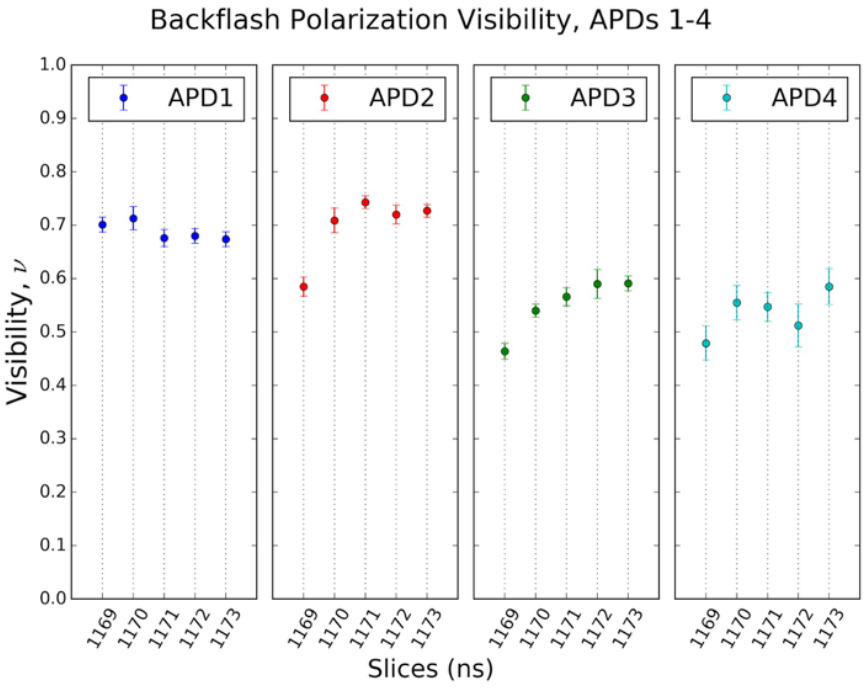


Figure 4: Visibility (ν) values for APDs 1-4. As backflashes are not always generated at the same time after the photodetection, they are detected by the backflash-detecting APD over a small range of times. Hence the five time "slices" for each APD.

Additionally, as APDs 1-2 and APDs 3-4 both correspond to two orthogonal basis states, we expect a phase shift of $\pi/2$ between the polarization angles associated with maximum measured backflash intensities from each pair. We also expect to, with the AD basis being the HV basis rotated by $\pi/4$, see a phase difference of $\pi/4$ between cross-basis APD pairs. Figure 5 shows the estimated phase values of each slice from all four APDs, relative to each other. This figure clearly shows four distinct phases, with one for each APD.

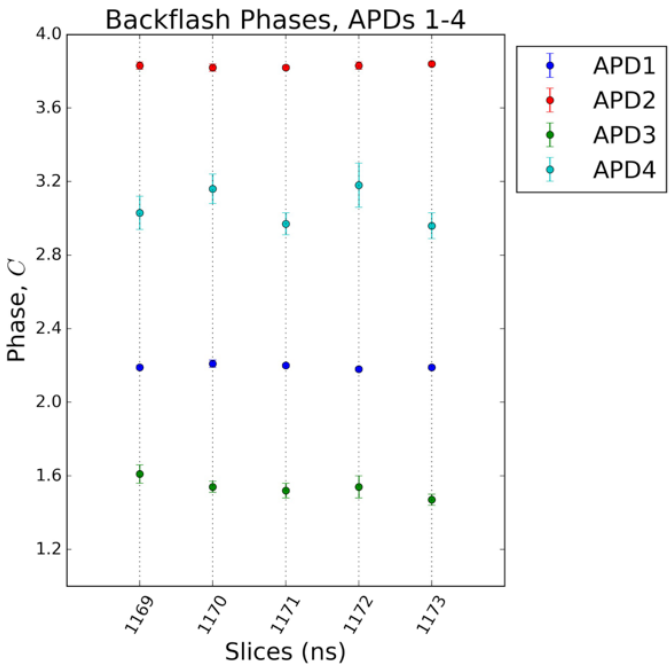


Figure 5: Phase values for each primary slice from APDs 1-4.

The data shows a clear correlation between the backflashes from individual APDs and their polarization. It appears that, with the appropriate resources, a hypothetical eavesdropper would be able exploit backflash polarization correlations to determine the originating APD, and therefore gain information regarding the result of the original BB84 measurement. This information leakage would not be detected by the legitimate communicators via the QBER, compromising QKD security.

While our quantitative results offer us confidence in reaching our conclusion, our nonideal visibility, distinguishability, and phase values reveal some flaws in our apparatus. This is partially attributed to issues such as backflash polarization distortion from the optics used, non-ideal beamsplitters, non-ideal circular polarization for the incoming photons from the BB84 source, varying detector efficiencies, and the fact that the HWP was not precisely calibrated.

In order to evaluate the practicality of the backflash attack, one needs to quantify the rate of information leakage due to backflashes. To do this, however, one needs to first determine the backflash rate and compare it to the rate of incoming photons. As one may conclude from the discussions in [6, 4], this value is dependent on a complicated convolution of several functions and parameters, including the capture efficiencies and backflash amplitudes of the primary APDs, the efficiency for the backflash coupling back into the quantum channel, fiber attenuation effects, and the efficiency of the backflash-detecting APD. Characterizing each of those effects must be relegated to future work.

While, without the backflash rate information, we cannot know with certainty, it may be the case that even if an eavesdropper Eve maximizes her detection efficiency with superior technology, the spectral and spatial filtering countermeasures described by Kurtsiefer et al. would reduce backflash levels such that Eve would gain very little information regarding the secret key. This information would then be reduced even further with privacy amplification procedures that the legitimate users perform to increase the security of their key. Furthermore, there are some emerging single-photon detection technologies that do not use avalanches in semiconductors, such as superconducting nanowire detectors [8] that may not exhibit backflash behavior.

As we have discussed, quantum key distribution (QKD) promises a theoretically unbreakable cryptosystem by employing the probabilistic nature of quantum measurement over mutually unbiased bases. In ideal conditions the security of QKD is guaranteed, even against quantum computers. Thus, QKD is one possible replacement for classical cryptosystems threatened by quantum computing.

However, we have also seen how non-ideal physical implementations of QKD systems render them vulnerable to various attacks that weaken their security, such as side channel attacks. We have considered the avalanche photodiode backflash side channel attack as an example. The results of the authors' experiment investigating this attack indicate that, if not properly addressed, QKD security could be compromised.

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. 74(1), 145–195 (2002).

[2] G. Brassard, N. Lu¨tkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," Phys. Rev. Lett. 85(6), 1330–1333 (2000).

[3] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full field implementation of a perfect eavesdropper on a quantum cryptography system," Nat. Commun. 2(1), 349 (2011).

[4] A. Spinelli and A. L. Lacaita, "Physics and numerical simulation of single photon avalanche diodes," IEEE Transactions on Electron Devices 44(11), 1931–1943 (1997).

[5] F. Acerbi, A. Tosi and F. Zappa, "Avalanche Current Waveform Estimated From Electroluminescence in InGaAs/InP SPADs," IEEE Photonics Technology Letters 25(18), 1778–1780 (2013).

[6] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes–back door for eavesdropper attacks?" J. Mod. Opt. 48(13), 2039–2047 (2001).

[7] A. Meda, I. P. Degiovanni, A. Tosi, Z. Yuan, G. Brida, and M. Genovese, "Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution," Light: Science and Applications 6(6), (2017).

[8] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," Nat. Photon. 3(12), 696–705 (2009).

[9] J. Katz and Y. Lindell, Introduction to Modern Cryptography, CRC Press, (2008).

[10] C.K. Shannon, "Communication theory of secrecy systems," The Bell System Technical Journal 28(4), 656–715 (1949).

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," Commun. ACM 21(2), 120–126 (1978).

[12] N. D. Mermin, Quantum Computer Science: An Introduction, Cambridge University Press (2007).

[13] A. Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," Rev. Mod. Phys. 68(3), 733–753 (1996).

[14] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134 (1994).

[15] T.D. Ladd and F. Jelezko and R. Laflamme and Y. Nakamura and C. Monroe and J. L. O/'Brien, "Quantum computers," Nat. 464(7285), 45–53 (2010).

[16] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Dec., 175–179 (1984).

[17] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nat. 299(5886), 802–803 (1982).

[18] A. Houck, "ELE 368: Introduction to Quantum Computing, Lecture on Quantum Key Distribution."

[19] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. 67(6), 661–663 (1991).

[20] R. Ursin and F. Tiefenbacher and T. Schmitt-Manderbach and H. Weier and T. Scheidl and M. Lindenthal and B. Blauensteiner and T. Jennewein and J. Perdigues and P. Trojek and B. Omer and M. Furst and M. Meyenburg and J. Rarity and Z. Sodnik and C. Barbieri and H. Weinfurter and A. Zeilinger, "Entanglement-based quantum communication over 144 km," Nat. Phys. 3(7), 481–486 (2007).

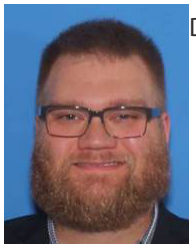
[21] E. Gibney, "Chinese satellite is one giant step for the quantum internet," Nat. News, Aug. (2016).

[22] H. Lo and M. Curty and K. Tamaki, "Secure quantum key distribution," Nat. Photon 8(8), 595–604 (2014).

[23] D. Stucki and M. Legr and F. Buntschu and B. Clausen and N. Felber and N. Gisin and L. Henzen and P. Junod and G. Litzistorf and P. Monbaron and L. Monat and J. B. Page and D. Perroud and G. Ribordy and A. Rochas and S. Robyr and J. Tavares and R. Thew and P. Trinkler and S. Ventura and R. Voirol and N. Walenta and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," New Journal of Physics 13(12) (2011).

[24] R. Newman, "Visible Light from a Silicon p-n Junction," Phys. Rev. 100(2), 700–703 (1955).

[25] S. Villa and A. L. Lacaita and A. Pacelli, "Photon emission from hot electrons in silicon," Phys. Rev. B 52(15) 10993–10999 (1995).



Dr. Brandon Rodenburg is a Senior Physicist and Quantum Information Scientist in MITRE's Physical Sciences, Nanosystems, & Quantum group at Princeton. He graduated college from Creighton University with a B.S. in physics, as well as B.S. major in mathematics. He received his Ph.D. from the University of Rochester's Institute of Optics, where he worked in experimental quantum optics studying the generation, propagation, and state discrimination of structured beams of light for applications in quantum information and communication. After finishing his graduate research, Dr. Rodenburg became a postdoctoral researcher working in the field of theoretical quantum optomechanics at the Rochester Institute of Technology. There he developed a quantum model of levitated nanoparticles and demonstrated that such systems could exhibit non-classical features which provided a completely new platform within quantum information science which may be exploited for such applications as quantum information processing or extremely sensitive force measurements. Dr. Rodenburg joined the MITRE Quantum Information Science group in the summer of 2016 and has been working to expand the depth and breadth of research both within quantum information and in a variety of other areas that are of importance to MITRE's sponsors.

Colin Lualdi received his A.B. in Physics from Princeton University in 2017. From 2015 to 2017 he worked as an intern for the Quantum Information Science group at the MITRE Corporation. He is currently pursuing his PhD in Physics at the University of Illinois, Urbana-Champaign. His research interests are primarily in the area of experimental photonic quantum information.

Dr. Daniel Stack is currently a Senior Research Scientist with Honeywell's Advanced Connected Sustainable Technologies Laboratory. Previously he has held positions at MITRE and as an ORAU Postdoctoral Fellow at the US Army Research Laboratory. In 2012 he received his Ph.D. in physics from Stony Brook University under the guidance of Distinguished Teaching Professor Harold Metcalf. His research interests include Quantum Optics and the laser cooling of atoms for Quantum Information Processing.

Quantum Teleportation: from Sci-fi to the Quantum Wi-fi

by: Daniel Cavalcanti and Paul Skrzypczyk

Travelling from one place to another without having to make the journey along the way is a science fiction dream immortalised in the famus Startrek's quote "Beam me up, Scotty!" [1]. In 1993 a group of six bright scientists showed that the rules of quantum physics allow for a very similar phenomenon, which they named quantum teleportation [2]. Their seminal paper quickly became recognised as a breakthrough in physics (it is the most cited paper in the field of quantum information). In the past 20 years, quantum teleportation has been implemented in a variety of physical setups, over distances of up to 1,400 kilometres, from a ground laboratory to a satellite [3].

Quantum teleportation is the process in which an unknown quantum state of a system S, held by a party customarily called Alice, is transferred to a system B, held by a party called Bob, who is in a far away location. In order to accomplish this task, Alice and Bob must share a pair of systems which are in a very special quantum state – known as a maximally entangled state (which serves as the physical 'channel' through which teleportation takes place) and Alice must communicate a small amount of additional classical information to Bob.

Mathematically, quantum teleportation can actually be easily understood, relying only on basic aspects of quantum theory. Suppose Alice has been given a system S in a generic quantum state $\Psi\rangle S = a\,|0\rangle + b\,|1\rangle$. Moreover, her and Bob share a bipartite system AB in a maximally entangled state $|\Phi\rangle AB = (|00\rangle + |11\rangle)/\sqrt{2}$. Using the famous superposition principle of quantum theory, it is possible to re-express the combined systems $|\Psi\rangle S\,|\Phi\rangle AB$ (1) as

$$
\begin{aligned}
|\Psi\rangle_S |\Phi\rangle_{AB} &= (a\,|0\rangle_S + b\,|1\rangle_S)\frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}} \\
&= \frac{1}{2}\frac{|00\rangle_{SA} + |11\rangle_{SA}}{\sqrt{2}}(a\,|0\rangle_B + b\,|1\rangle_B) \\
&+ \frac{1}{2}\frac{|00\rangle_{SA} - |11\rangle_{SA}}{\sqrt{2}}(a\,|0\rangle_B - b\,|1\rangle_B) \\
&+ \frac{1}{2}\frac{|01\rangle_{SA} + |10\rangle_{SA}}{\sqrt{2}}(b\,|0\rangle_B + a\,|1\rangle_B) \\
&+ \frac{1}{2}\frac{|01\rangle_{SA} - |10\rangle_{SA}}{\sqrt{2}}(b\,|0\rangle_B - a\,|1\rangle_B).
\end{aligned}
\tag{1}
$$

What this mathematical identity shows is that if Alice applies a measurement on her systems S and A corresponding to the projections onto the states $(|00\rangle+|11\rangle)/\sqrt{2}$, $(|00\rangle-|11\rangle)/\sqrt{2}$, $(|01\rangle+|10\rangle)/\sqrt{2}$, and $(|01\rangle-|10\rangle)/\sqrt{2}$ (this special measurement is called a Bell state measurement) Bob is automatically left with one of the four states $a\,0\rangle + b\,|1\rangle$, $a\,|0\rangle - b\,|1\rangle$, $b\,|0\rangle + a\,|1\rangle$ or $b\,|0\rangle - a\,|1\rangle$ Notice that the first state is in fact already the original state $|\Psi\rangle$ that Alice wants to teleport to Bob, while the other three can be transformed into $|\Psi\rangle$ by appropriate transformations ($|1\rangle \to -|1\rangle$, $|0\rangle \leftrightarrow |1\rangle$, or both). In other words, Alice applies a measurement to her systems S and A, and, conditioned to the outcome she observes the system of Bob will acquire a state that is the same as the original state of S after an appropriate correction. Bob doesn't know which correction, if any, to make until he learns the result of Alice's measurement, which is exactly what she must communicate to him.

There are a number of important aspects worth noting about quantum teleportation. First, unlike the sci-fi idea of disappearing here and appearing there, in quantum teleportation it is not the physical system that is transferred from one place to another, but only its state. This is actually very interesting, because systems S and B can actually be completely different types of physical systems! For example photons and atoms [4]. Second, due to the classical

message that needs to be sent to Bob in order for him to make the correction, quantum teleportation is not accomplished instantaneously, but rather takes time to complete – the time it takes for the communication to travel to Bob, which cannot travel faster than the speed of light. A final fascinating aspect is that once the state of S is teleported to system B, $S's$ state changes completely. In fact, it contains absolutely no information

about the state prior to teleportation whatsoever. This is crucial, since it ensures that in the end there will not be two copies of the same state. This in itself is another deep and important property of quantum theory – unlike classical information that can be copied at will, copying an unknown quantum states is actually forbidden [5]).

Although very simple on paper, actually demonstrating teleportation in the laboratory is very difficult. First of all, it requires Alice and Bob to share systems in a maximally entangled state, over large distances. Entanglement is however a very fragile quantum property that quickly deteriorates in practice, and hence huge efforts have to be made to generate and distribute the entanglement necessary for teleportation. Second, Alice has to be able to make the joint Bell state measurement on her systems S and A. This measuremnt is also particularly demanding, requiring extremely precise interactions to be engineered and controlled by individual atoms or photons. Finally, Bob has to wait until he recieves the message with the result of Alice's measurement, before he knows how to correct his state accordingly, the whole while protecting his system from external sources of noise which 2 again destroy and decohere its fragile quantum state.

It was a 4 year race before the first experimental group managed to overcome the above obstacles and finally demonstrate quantum teleportation. All of the first demonstrations were realised using photons [6–8]. Soon after, it was also demonstrated using atoms, nuclear magnetic resonance (NMR), and solid-state sysytems [9]. By now it has been demonstrated using a huge array of different setups.

One important fact about quantum teleportation is that it can be used as a building block to accomplish other tasks in quantum

information. As a first example, if the system S is itself entangled with a system S' held by another far away party (let's call them Charlie), then after teleportation has been performed, the systems S' and B will end up in an entangled state – even though they were never in the same place. This is known as entanglement swapping and is a method of generating entanglement between distant systems (Bob and Charlie) by performing a measurement at an intermediate location (Alice's laboratory). This process is the basis of a so-called quantum repeater, which is a leading candidate method for building future large-scale quantum networks which might one day span the planet. As a second example in which quantum teleportation can play a role is in quantum computing – a computer which replaces bits with two-state quantum systems, referred to as qubits. This however is another to-become-reality-sci-fi story!

REFERENCES

[1] https : ==en:wikipedia:org=wiki=Beam me up; Scotty.

[2] C. H. Bennett, G. Brassard, C. Cr´epeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett. 70, 1895 (1993).

[3] Ji-Gang Ren et al., Ground-to-satellite quantum teleportation, Nature 549, 70 (2017).

[4] J. F. Sherson, et al., Quantum teleportation between light and matter, Nature 443, 557 (2006).

[5] W. K. Wooters and W. H. Zurek, A single quantum cannot be cloned, Nature 299, 802 (1982).

[6] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels Phys. Rev. Lett. 80, 1121 (1998).

[7] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H.Weinfurter, and A. Zeilinger, Experimental quantum teleportation, Nature 390, 575-579 (1997).

[8] A. Furusawa, et al. Unconditional quantum teleportation, Science 282, 706709 (1998).

[9] S. Pirandola, J. Eisert, C.Weedbrook, A. Furusawa, and S. L. Braunstein, Advances in quantum teleportation, Nature Photonics 9, 641652 (2015).

Daniel Cavalcanti is a research fellow in the Quantum Information Theory Group at ICFO-The Institute of Photonic Sciences (Barcelona, Spain). He obtained his PhD in physics from the Universisty of Barcelona in 2008, and subsequently worked as a Postdoctoral Researcher in the Centre for Quantum Technologies in Singapore until 2013. Daniel Cavalcanti is also a graphic designer

Paul Skrzypczyk is currently a Royal Society University Research Fellow at the University of Bristol. Prior to this, he worked in the group of Antonio Acin at ICFO - The Institute of Photonic Sciences, Barcelona, between 2013 and 2015, and in the group of Richard Jozsa at the University of Cambridge between 2011 and 2013. Paul obtained his PhD from University of Bristol, under the supervision of Sandu Popescu, from 2007 to 2011. He completed an MPhys in Theoretical Physics at University of Sussex from 2003 to 2007.

2018 IEEE-HKN Awards

CALL FOR NOMINATIONS

Deadlines Start: 7 May 2018

IEEE-Eta Kappa Nu (IEEE-HKN) has numerous award programs designed to promote and encourage educational excellence in electrical and computer engineering. These awards recognize outstanding accomplishments by students, professors, and industry professionals who make significant contributions to society, and who exemplify a balance of scholarship, service, leadership, and character. IEEE-HKN encourages Chapters and individuals to nominate all eligible candidates.

For IEEE-HKN Awards information and instructions for submitting a nomination, visit **https://hkn.ieee.org/get-involved/awards/**.

Vladimir Karapetoff Outstanding Technical Achievement Award
Nomination Deadline: 7 May

Distinguished Service Award
Nomination Deadline: 7 May

Outstanding Young Professional Award
Nomination Deadline: 7 May

Outstanding Teaching Award
Nomination Deadline: 7 May

Alton B. Zerby and Carl T. Koerner Outstanding Student Award
Nomination Deadline: 30 June

Outstanding Chapter Award
Nomination Deadline: 30 September

NOW ACCEPTING NOMINATIONS

DEADLINES START: 7 MAY 2018

https://hkn.ieee.org/get-involved/awards/

Check Out One of the Best Awards you've Never Heard of

Are you jazzed about networking with the people who created the ground-breaking technologies that we all rely on today - like Vint Cerf, Marty Cooper, Len Kleinrock, Brad Parkinson and others?

Do you want to be part of a peer group of the most promising networking and communications engineers in the world?

Does the credibility that comes with international recognition for your best work sound like something that would help your career?

If so, read on!

Young Scholars at Marconi Society Gala

The Marconi Society is a foundation dedicated to advancements in the Internet and communications that benefit humankind. Each year, we select a small group of Paul Baran Young Scholars from a competitive set of nominations. We will accept nominations for the 2018 Young Scholars from February 1 through June 30, 2018.

Being honored as a Young Scholar is often an early step in continued recognition in the field. Our Young Scholars are named to the Forbes 30 Under 30 list. They are recognized as Global Young Leaders by the World Economic Forum. They receive additional IEEE awards such as the Outstanding Young Professional Award. In each case they say that becoming a Marconi Society Young Scholar helped them stand out among highly credible contenders.

Marconi Society Young Scholars work in industry, in academia and are entrepreneurs leading highly innovative companies. In addition, Young Scholars are mentored by and network with the Marconi Fellows, engineering leaders who developed the Internet, wireless, GPS, digital video and network security, to name just a few key technologies.

The Young Scholars are committed to positive social impact and created the Celestini Program to directly support and mentor engineering students in developing countries. By teaming with students to solve problems that are important on a local level, the Young Scholars have supported applications to improve the health of expectant moms in Uganda and to reduce pedestrian traffic deaths in Delhi. New projects start each year.

If this sounds like a good fit for you or a researcher you know, here are the details:

We look for nominations of creative and entrepreneurial researchers who show the potential to make extraordinary contributions to the field of information and communications science.

In addition to rewarding relationships with the best in the field, awardees receive a $4,000 cash prize and travel expenses to attend the annual Marconi Society Symposium and award recognition dinner (to be held this year in Bologna, Italy.).

Candidates must be nominated, typically by a professor or research advisor.

Meet the Young Scholars and, if you like what you see, make sure that your nomination is in by June 30, 2018.

If you're not sold yet, here's what some of the Young Scholars have to say:

"I am humbled and honored to be chosen for the Young Scholar Award. It is easier to be known in your own area, but the fact that the award helps my work translate to broader audiences in the communications arena makes me very proud. It gives me assurance that I'm moving in the right direction."

Negar Reiskarimian, 2017 Young Scholar, PhD Candidate at Columbia University

"I found the award indispensible in establishing myself and making connections. The publicity generated from the award provided a platform to share my research and form potential collaborations."

Joe Lukens, 2015 Young Scholar, Wigner Fellow at Oakridge National Laboratory

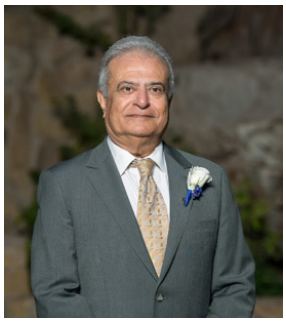
"Being a Young Scholar has given me a broad perspective on how one should do their research, taking more risk and focusing on a longer timeframe. The Marconi Fellows took huge risks in their careers, which clearly paid off."

Rafael Laufer, 2008 Young Scholar, Quantitative Software Engineer at Two Sigma

Marconi Society 2017 Young Scholars

We seek a diverse and innovative set of nominees. Please contact us at info@marconisociety.org with questions. We look forward to seeing your nomination!

IEEE-HKN 2017 Awards Ceremony Updates



Life Fellow Asad M. Madni is the recipient of the honor society's Vladimir Karapetoff Outstanding Technical Achievement Award "for seminal contributions to the development and commercialization of intelligent microsensors for aerospace, commercial aviation, and automotive safety." Until Madni retired in 2006, he was president, chief operating officer, and chief technology officer of BEI Technologies, in Thousand Oaks, Calif. There he led the development and commercialization of intelligent sensors and systems for the aerospace and transportation industries. Today he is a consultant and an adjunct professor at the University of California, Los Angeles, as well as executive managing director and CTO at Crocker Capital, in San Francisco.

The C. Holmes MacDonald Outstanding Teaching Award was given to Senior Member Siddharth Suryanarayanan "for leadership and excellence in curriculum design, course delivery, and the education and mentorship of electric power engineers." Suryanarayanan is an associate professor in the electrical and computer engineering department at Colorado State University. He has designed, developed, and taught four graduate-level courses in electric power systems engineering and has created an online graduate certificate program for the university. In recognition of his contributions, the university awarded him the Lisa and Desi Rhoden Endowed Chair, the first endowed professorship in the department's history. Suryanarayanan is vice president of the IEEE Power & Energy's education committee.

IEEE-HKN member Jamal Madni was named the society's Outstanding Young Professional "for contributions in software engineering and technology advocacy." Madni is a program manager and chief architect of special projects within Boeing Satellite Systems, headquartered in El Segundo, Calif. He leads the execution of the integrated electronics suite in collaboration with NASA and the Indian Space Research Organization. He also serves as chief architect system, a software intelligence package designed to emulate biomedical applications. For his efforts, he received the 2017 Boeing World-Class Engineering Award in Growth as well as the company's employee engagement association project for this year.

Fellow John Orr received the Meritorious Service Citation "in recognition of sustained contributions and leadership in IEEE-HKN and engineering accreditation." Orr is professor emeritus of electrical and computer engineering at Worcester Polytechnic Institute, in Massachusetts. He is past president of IEEE-HKN and former chair of the ABET Engineering Accreditation Commission.

Richard Feynman's "There's Plenty of Room at the Bottom" Talk

by: Doug Tougaw

Richard Feynman (1918-1988) was one of the most prolific and well-known physicists of the 20th century. His work in superfluidity, quantum electrodynamics, and quantum gravity set the course of much of the research that has followed since. He was recognized with a Nobel Prize in Physics in 1965 for his work in quantum electrodynamics. Perhaps even more importantly, his pedagogical work influenced generations of future physicists and engineers. The Feynman Lectures on Physics were (and still are) the first and best exposure that many Eta Kappa Nu members had to fundamental ideas of mechanics, electromagnetism, and quantum mechanics.

In 1959, Dr. Feynman presented a talk to the American Physical Society in Pasadena entitled, "There's Plenty of Room at the Bottom." In this talk, he outlined the physical limitations of what we now know as nanotechnology or quantum engineering, and he was among the first to point out just how small things could really get. By performing calculations that were accessible to any undergraduate student, he pointed out that it would be possible to write the entire Encyclopedia Britannica on the head of a pin and still have approximately 1000 atoms within each dot in a half-tone reproduction. Such a dot would be about 8.5 nm in diameter—startlingly close to the 7-10 nm minimum feature size that is the current state of the art. He followed this prediction by calculating that all of the information published in all of the books in the world (up to 1959) could be stored in a cube of material one two-hundredth of an inch on each side, "the barest piece of dust that can be made out by the human eye."

Dr. Feynman was also able to bring in biological comparisons to DNA sequences and brain structure to prove that high-density information storage and computational power had already been demonstrated by nature. His thesis seems to be that if it has already been done by nature, then eventually humanity will be able to do it, too.

By combining a thorough knowledge of the physical limitations of matter with an optimism for human ingenuity, Dr. Feynman predicted a majority of the incredible progress that has been made in the nearly 60 years since his talk.

It would be nice to say that his talk provided a roadmap that guided scientists and engineers working over the next several decades to achieve his vision. Unfortunately, his talk did not receive the attention it deserved at the time, and it was only in the 1990s when it was re-discovered and its propositions were verified in hindsight. It makes one wonder how many other works like this one are just waiting for us to re-discover them in the historical archives.

Full text of Feynman's Talk:
http://www.its.caltech.edu/~feynman/plenty.html

2016-2017 Outstanding Chapter Awards Announcement

The IEEE-Eta Kappa Nu (IEEE-HKN) Board of Governors has conferred on the following IEEE-HKN Chapters the 2016-2017 IEEE-HKN Outstanding Chapter Award:

Chapter Name	University
Alpha Chapter	University of Illinois at Urbana Champaign
Beta Alpha Chapter	Drexel University
Beta Chapter	Purdue University
Beta Epsilon Chapter	University of Michigan
Beta Kappa Chapter	Kansas State University
Beta Lambda Chapter	Virginia Polytechnic Institute and State University
Beta Omega Chapter	University of Connecticut
Beta Theta Chapter	Massachusetts Institute of Technology
Delta Epsilon Chapter	Ohio University
Delta Omega Chapter	University of Hawaii at Manoa
Gamma Delta Chapter	Worcester Polytechnic Institute
Gamma Tau Chapter	North Dakota State University
Gamma Theta Chapter	Missouri University of Science and Technology
Iota Chi Chapter	Oakland University
Iota Gamma Chapter	University of California, Los Angeles
Iota Zeta Chapter	California State University, Chico
Kappa Psi Chapter	University of California, San Diego
Lambda Sigma Chapter	University of California, Riverside
Mu Alpha Chapter	UCSI University
Mu Chapter	University of California, Berkeley
Mu Iota Chapter	Seattle University
Mu Nu Chapter	Politecnico di Torino
Nu Chapter	Iowa State University
Zeta Beta Chapter	Texa A&M University, Kingsville

This award is presented to IEEE-HKN Chapters in recognition of excellence in their Chapter administration and programs. Service to the community and others is an expectation of IEEE-HKN Chapters.

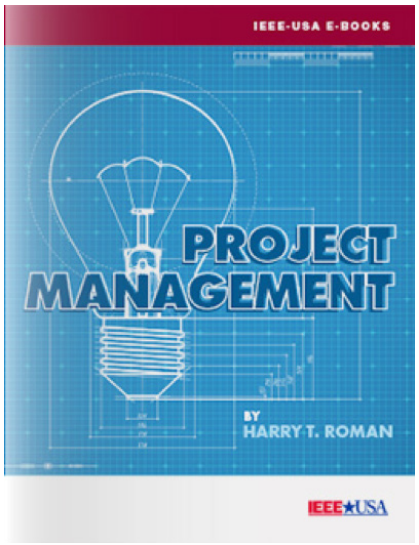
Recipients are selected on the basis of their annual Chapter report. Winning Chapter reports showcase their Chapter's activities in an individualized manner and provide multiple views and instances of their work, which really brings their Chapter's activities to life. Of critical concern to the Outstanding Chapter Awards evaluation committee in judging a Chapter are activities to: improve professional development; raise instructional and institutional standards; encourage scholarship and creativity; provide a public service; and generally further the established goals of IEEE-HKN.

The awards will be presented at a special reception held on19 March 2018, in conjunction with the Annual Electrical and Computer Engineering Department Heads Association (ECEDHA) meeting; in Monterrey, California. At the Awards Dinner immediately following the reception, the 2017 Alton B. Zerby and Carl T. Koerner Outstanding Student Award will be presented to Katelyn Brinker of the IEEE-HKN Gamma Theta Chapter at Missouri University of Science & Technology, and James Smith of the IEEE-HKN Xi Chapter at Auburn University.

IEEE-USA Free Ebook!

by: Harry T. Roman

Through 15 February, IEEE members can download a free copy of this eBook by adding it to your cart and using promo code JANFREE18 at checkout.



Project management skills are highly prized in any organization. Engineers who can develop new plans for critical corporation products, services, internal process improvements and special needs technologies; and then coalesce, manage and lead others to make these things happen, are never going to fear unemployment. And they are going to have a great time working on interesting, innovative, and sometimes groundbreaking, projects. Project management is probably the most important function young engineers can learn, along with an ability to articulate the value of what they, and their teams, are doing.

ABOUT IEEE-USA

IEEE-USA is an organizational unit of the Institute of Electrical and Electronics Engineers, Inc. (IEEE), created in 1973 to support the career and public policy interests of IEEE's U.S. members. IEEE-USA is primarily supported by an annual assessment paid by U.S. IEEE Members.

Through its products and services, IEEE-USA serve as a resource for enhancing the professional growth and career advancement of U.S. IEEE Members. And through its Government Relations programs, IEEE-USA works with all three branches of the federal government to help shape the workforce and technology policy to the benefit of members, the profession and the American public.

Board of Governors Election Results 2018

IEEE-HKN is proud to announce the election of new President-Elect and Governors who took office on 1 January 2018.

President Elect
Karen Panetta

Governor at-Large
James Conrad

Region 1-2 Governor
Sean Bentley

Governor at-Large
John DeGraw

Region 5-6 Governor
Rakesh Kumar

Student Governor
Kathleen Lewis

For more information about the 2018 IEEE-HKN Board of Governors, please visit us at this link!

Epsilon Xi: Go Baby Go!

EPICS in IEEE recently awarded its first project for 2017 to the Epsilon Xi Chapter of IEEE-HKN at Wichita State University, Wichita, KS, USA for a project titled "Ride- on Cars for Children with Disabilities (Go-Baby-Go)". The project brings together the IEEE-HKN Chapter with 40 high school students and 10 IEEE volunteers from the area to develop low-cost, high-impact technologies designed to address the specific needs of a particular child whether it be for toy cars for infants or hands- free harness systems for children with mobility impairments.

BACKGROUND:

Why is Go Baby Go Such an Important Project?

As soon as children begin to crawl, walk, and run, they begin to explore their surroundings. They learn about the world around them and objects in it. Their mobility motivates them to do more and to continue learning on a daily basis. Children with physical disabilities that limit mobility lag in this form of development. Research has shown that independent mobility positively impacts motor, cognitive, language and social-emotional development, particularly from birth to five years of age [1]. Being pushed in a stroller or being carried from one place to another is fundamentally different from having active control over one's own exploration, which is where developmental gains are seen. The use of a mobility aid that a child can control can help to eliminate these impairments [2].

The modified ride-on cars do more for the children than just granting them mobility; children who achieve self-directed mobility, whether on their own or using some sort of assistive device, experience more social interactions, which lead to better communication skills. By combining electrical and

computer engineering with community engagement, we are creating accessible, personalized vehicles that enable independent mobility in real-world environments. There are few commercially available devices for children with mobility issues to move around on their own. Powered wheelchairs usually are not an option for very young children.

Manual wheelchairs can also be prohibitive. The modified toy cars provide them independence at a much younger age and at a fraction of what a powered wheelchair would cost. The current number of children in Sedgwick and Butler counties receiving services from Rainbows United is approximately 3500. This includes children receiving services for motor delays [3]. Therefore, a significant percentage of these children would benefit from WSU IEEE-HKN Go Baby Go. Young children beyond the age of three may also benefit from modified ride-on vehicles. If our program receives funding at the level we desire, we guarantee that numerous families with needs will receive our products.

Project Objectives:

1. Provide mobility to children with physical disabilities that otherwise impair independent mobility.

1.a. Enhance the technology utilization in the ride-on vehicles while ensuring they are safe and secure for children below the age of five.

1.b. Plan and prepare the ride-on vehicles while addressing the specific needs of individual children.

1.c. Educate parents on the basic use and troubleshooting of the modified ride-on vehicles.

2. Introduce high school students to science, technology, engineering, and mathematics (STEM) disciplines as well as show how these technologies can benefit the community. At the same time, give these school children an opportunity to engage in community service.

3. Continue to promote the open-sourcing of methods used in designing ride-on vehicles and increase the project impact.

3.a. Document all technology being implemented on these vehicles.

PROFESSIONAL PROFILE:

James A. Jefferies

2018 IEEE President and CEO
Beta Psi Chapter

Jim Jefferies retired from AT&T and Lucent Technologies following 33 years in engineering and executive positions including fiber optic cable development and manufacturing, quality assurance, and supply chain management. He managed the engineering teams that delivered the first commercial fiber optic cables for AT&T. He served as logistics vice president, responsible for worldwide supply chain and export planning. He has led teams in major technology transfers, transitions of information technology, and organizational change. He has also worked in the entrepreneurial sector as Chief Operating Officer for USBuild.com in San Francisco, CA, USA.

Jim served two separate terms on the IEEE Board of Directors, as well as 2015 IEEE-USA President. As President of IEEE-USA, Jim supported the expanded focus on public visibility, young professionals, and humanitarian outreach.

He received his BS in Electrical Engineering from the University of Nebraska and an MS in Engineering Science from Clarkson University. He attended the Stanford University Graduate School of Business as a Sloan Fellow and earned an MS in Management.

Jim is a licensed professional engineer (Emeritus).

MY INDUCTION INTO ETA KAPPA NU

My connection to HKN dates back to 1968 as a student in electrical engineering at the University of Nebraska. I was not that aware of the organization or the membership invitation process. I lived off campus and often grouped classes, but we all came together for EE classes in good old Ferguson Hall. One evening, near the start of the term, a few members came to my fraternity house with a message that I had been selected. They said it was good that I had finished a strong semester because they had been watching me. What more needs to be said about an organization that is dedicated to community, service, and leadership. I was soon off to military service, but always remember the HKN connection and pride in carrying it on my resume for almost 50 years.

There was one other little requirement for new inductees -- I was given a blank piece of wood and a list of names of all the members, faculty, alumni, and fellow inductees of the Beta Psi Chapter. The assignment was to find them, meet them, and get their personal signature on the plaque. There were class hours and office hours but no "find the professor app" around.

The photo above is that hand-painted plaque which I still have with more than 70 signatures. It was all a great experience.
https://www.youtube.com/watch?v=D8CexXR7iRs&feature=youtu.be

Why did you choose to study the field of engineering (or the field you studied)?

Seemed like electrical engineer was always in my future. Growing up in the space race era with a national priority on science and engineering, it was an easy fit. My father was a licensed professional engineer, although he did not have a college degree. I used to help him grade papers from the class he taught at the local university and he always supported my tinkering. My uncle was a machinist who had moved to California from the industrial Midwest to work on rocket engines; no other path was going to work.

What do you love about the industry?

As a manufacturing engineer, every day held a new challenge and learning opportunity. Materials, process, and people all came together in an elusive chase for the perfect quality part or system. There was always a next improvement and a strong team trying to get there.

What don't you like about the industry?

I dislike when manufacturing becomes viewed as a cost burden to a business rather than an integral part of creating value. My experience in the early introduction of fiber optic cable with overlapping research, development, and deployment was a memorable experience.

How has the field of engineering changed since you entered it?

Engineering training was more generalist with a goal to introduce many basic topics as a foundation for additional learning and with more direct lines of specialty. Today, access to information, supporting equipment, and people allow applicability of "engineering skills" across so many specialized fields and businesses. I think it's a great time to be an engineer embracing the many options available.

In what direction do you think that engineering and other IEEE fields of interest are headed in the next 10 years?

I think that engineering and other fields of interest are headed toward convergence. Progress in many fields will only be achieved in multidisciplinary teams whether Big Data driving medicine and agriculture or cloud computing integrating the data, education, and entertainment streams of daily life. Continued emphasis on improved inclusion and diversity in the profession will build the super teams that will be needed.

I see an increasing emphasis for the social impact of technology on humanity in addressing global challenges. That may be defined in directional documents like the United Nations sustainable development goals or the grand challenges of the National Academies and others. The awareness will grow and translate into early design state decisions considering ethics, sustainability, and bringing the promise of technology and economic opportunity. These are also some of the goals of IEEE.

What is the most important lesson you have learned during your time in the field?

Trust and respect the contributions of everyone. In building organizations, how you treat people in achieving results is equally as important as the results themselves.

What advice can you offer recent graduates entering the field?

Be bold in seeking new opportunities. There is learning and experience in every assignment. Be the one who really made something where others may not have seen it and share openly with others. If you have an interest, pursue it and be sure to let others know. Opportunities are not predictable, but preparation and looking in the right place helps. Don't underestimate the value of soft and interpersonal skills.

Finish this sentence. "If I had more time, I would …"

Prune the roses a little more carefully.

STUDENT PROFILE:

Silvia Vitali

Mu NU Chapter

Silvia Vitali earned her bachelor's degree in Computer Engineering at Politecnico di Torino and is currently studying for her Masters in Software Engineering. During the first term of the Academic Year 2016-2017, she and other students had managed to create the first initial group of founders of the future IEEE-HKN Mu Nu at Politecnico di Torino. In March 2017, with the Installation and Induction Ceremony the Mu Nu Chapter was officially founded and Silvia was named its President. Now, a new generation of officers is leading the Chapter, organizing new amazing and interesting activities.

What has it meant to you to be inducted IEEE-HKN?

Becoming part of the IEEE-HKN network has been an honor and a pleasure. In my case, my Induction was the same day as the Installation Ceremony. It was a very important day for my Chapter: after having worked for months creating in our university a new community based on IEEE-HKN principles, we managed to officially start it. The process that led to the installation ceremony has been long and sometimes difficult, but this just made that day more special. We planned the Installation Ceremony for months, and when finally that day came, it was exciting and touching to see our small community becoming part of the great IEEE-HKN family; and in the presence of many important academic personalities. On that day, we had finally reached our goal, but that was just the beginning of a new and amazing adventure.

Do you have a best HKN story to share (example: favorite program or activity)?

It is very difficult to choose just one HKN story. In just one academic year, so many things happened, and I took part in so many interesting situations that it is difficult to select a single episode. Despite the different public and private formative events we have organized, I would like to tell a different story, one of the HKN moments I will always remember fondly. It was a day we decided to organize a picnic together. After joking about the idea to have a lunch together in one of the main parks of Turin, we finally decided to put this idea into practice. We found a day in which almost all Chapter members were present, we cooked many different delicious dishes, we brought guitars, blankets and a ball. Everything was ready, but when the chosen day arrived, a few minutes after we got to the park, it started to rain! What an unlucky day! In few seconds all Chapter members were standing in the pouring rain, freezing in the blankets that were already soaked. However, this day is one of the most grateful memories I have related to my Chapter…after few minutes we found a covered place to wait out the rain and after a while, the sun came back, allowing us to continue to enjoy our day. In the end, it was amazing! We had the possibility to talk about future projects and Chapter activities in a relaxed way, and we started to create a strong bond that now still connects us.

Why did you choose to study the engineering field?

I like the idea to create something new, to bring to life things that are not real yet. I started to be interested in the engineering field because I thought it can help me to reach this goal, and the more I discovered about it, the more I was determined

to study engineering. Then, when I discovered computer engineering, I immediately knew I chose the right path because it gives you the possibility to create something new in a completely different and powerful way.

What do you love about engineering?

What I love more about engineering is the way in which the minds of people practicing and studying engineering is constantly trained to work in a logical way. Our mind is a powerful tool, but we need to keep practicing to maintain its training. The study of engineering helps us to do this; it is a way to always challenge ourselves and improve our skills and our way of thinking. A good engineer knows that his/her life and work is based on continuously learning something new. Learning is not something we have to do, it's something we actually like.

What is your dream job?

I don't really have a dream job, but I know which are the main aspects of my ideal job. I aim to do something constantly new and I'm scared of boring, monotonous jobs. I really hope to find something challenging and inspiring. I'm looking for that kind of job that makes you wake up every day looking forward to going to work and being productive. I strongly believe that if you do what you like you can be more efficient and you don't feel the fatigue.

Whom do you admire (professionally and/or personally) and why?

Elon Musk is one of the people I admire more. He is a great inventor, who was able to answer many of today's challenges in science and bring his unbelievable ideas to life. His qualities I admire most are his passion and curiosity, that have always pushed him to try and to learn, going well beyond the knowledge acquired at university. I'm also really impressed by his courage; he left his Ph.D. at Stanford University after two days and took the risk to follow his intuitions on new possible entrepreneurial ideas. Sometimes it is really difficult to take action, but we need to do it to achieve results never reached before. Finally, I admire his efficiency; he is able to immediately apply newly acquired knowledge and he can organize his time to perfectly keep up with the different companies he founded and other commitments he has. He teaches us that to reach our goals, we have to believe in ourselves and in our ideas and that it is important to be organized and focused. However, despite his intelligence and his capacities, his brilliant intuitions have been crucial to reach success…it is always important to think to new solutions, explore new research fields and try paths not taken by others.

What is the next BIG advance in engineering?

Engineering is a vast topic that is constantly developing. There are always new challenges in this field, and its changing nature makes it extremely difficult to think only about a single next possible advance. However, one field that has already seen interesting progress, and that will surely develop in the next future, is Artificial Intelligence. Last year, our Chapter organized a series of events on chatbots, with a particular interest in Natural Language Processing. NLP is the study of how machines can process human ("natural") language. It has different kinds of application, from language translation to automated customer relationship management and it is a specific field of Artificial Intelligence. The possibility to go deep into this field with experts from different companies, allows us to see which advances have been done and understand what is still missing. With this background, it is easier to understand which are the main challenges in the AI field. However, there is always new progress, and one day we'll probably hear about a machine which passed the Turing Test and is, or at least seems to be able to think.

IEEE-HKN Mu Nu Chapter, Politecnico di Torino, Torino, Italy

What is the most important thing you've learned in school?

One of the most important things I have learned from school is to be curious. The best teachers I have ever met are the kind of people that encourage students to ask questions, to investigate further class topics and look for new answers. I think it is important to maintain this attitude also in your future job to reach planned goals and good results.

What advice would you give to other students entering college and considering studying your major?

The first years at university can be very tough, especially in the field of computer engineering. My advice is to spend time during your first years investigating this complex field. In the future, you will be grateful you took your time to learn; you'll be able to apply your knowledge to reach new goals. Don't be afraid to learn something more than the university daily lesson; you need to study for your future and for yourself, not just to pass the exam. Finally, allow yourself to experiment. When you start working, you'll regret all the things you haven't done during your university life. This is the right time to learn a new programming language… to do that project you have kept in your mind one day too many…to go to conferences on topics you are interested in…and to discuss with people about your fields of interest to broaden your knowledge.

New and Reactivated Chapters

IEEE-HKN is proud to welcome two new chapters:

- Mu Omicron Chapter at Christopher Newport University, Virginia
- Mu Xi Chapter at the Indian Institute of Science, Bangalore

Congratulations to both chapters! And we hope to welcome you at all upcoming events and gatherings!

Inductees at Mu Xi Chapter, Indian Institute of Science

Inductees at Mu Omicron Chapter, Christopher Newport University

Share Your IEEE-Eta Kappa Nu Pride

Official Society Merchandise Now Available

Medal $20	Honor Stole $20
Three Pin Types:	Honor Chord . . . $30
Crest $12	6" Table Covers . $99
Emblem $12	Key Pendant . . . $14
Key $12	Scarf $22
	Necktie $25

Save $10 by purchasing the "honor combo" one honor cord and one honor stole for $40

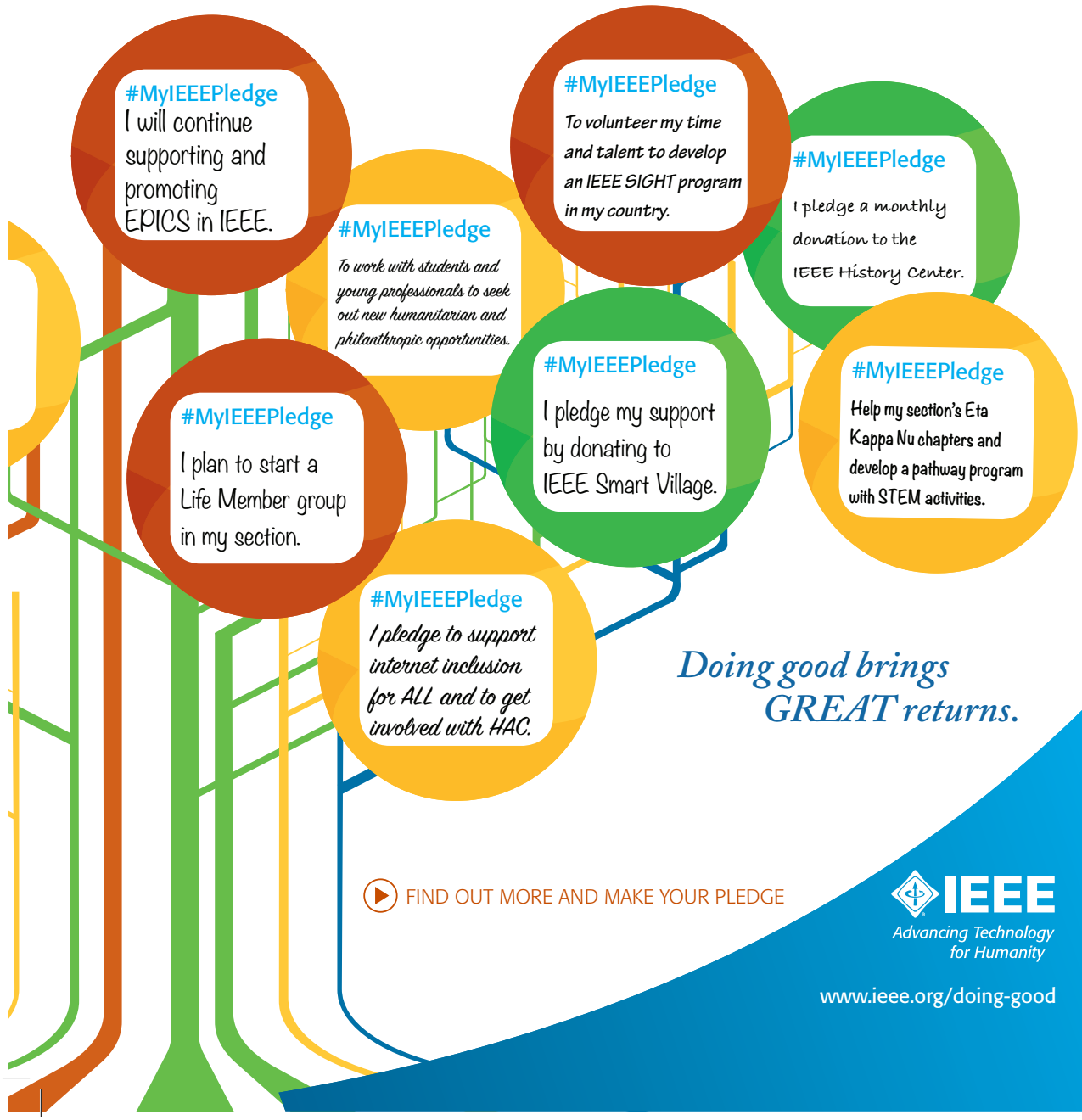
Save $21 by purchasing 10 of the same style pin for $99

All items available at the IEEE-HKN store at:
bit.ly/IEEEHKNstore

IEEE
Advancing Technology for Humanity

IEEE Humanitarian & Philanthropic Opportunities

You can help advance technology for humanity by contributing your time, talent, and/or treasure to the diverse menu of IEEE humanitarian and philanthropic opportunities. Leverage the strength and reach of the IEEE network to make a difference worldwide.



Doing good brings GREAT returns.

FIND OUT MORE AND MAKE YOUR PLEDGE

IEEE
Advancing Technology for Humanity

www.ieee.org/doing-good