Practical Quantum Communication and Cryptography for WDM Optical Networks

Prem Kumar

Center for Photonic Communication and Computing, Department of Electrical and Computer Engineering and Department of Physics and Astronomy, Northwestern University, Evanston, IL 60208-3118

Abstract.

Keeping in mind the ubiquitous standard optical fiber for long-distance transmission and the widespread availability of efficient active and passive fiber devices, we have been developing telecom-band resources for practical quantum communication and cryptography in wave-division-multiplexed (WDM) optical networks. In this talk I present our recent results on two fronts: i) telecom-band in-fiber entanglement generation, storage, and long-distance distribution and ii) quantum-noise protected high-speed data encryption through an optically-amplified WDM line. Along the first front, with our in-fiber entanglement source all four Bell states can be readily produced and we have demonstrated violation of Bell’s inequalities by up to 10 standard deviations of measurement uncertainty. With such a source we have demonstrated storage of entanglement for up to 1/8 of a millisecond. Furthermore, when each photon of the entangled pair is propagated in separate 25km-long standard fibers, high visibility quantum interference is still observed, demonstrating that this system is capable of long-distance (> 50 km) entanglement distribution. Along the second front, we have implemented a new quantum cryptographic scheme, based on Yuen’s KCQ protocol, in which the inherent quantum noise of coherent states of light is used to perform the cryptographic service of data encryption. In this scheme a legitimate receiver, with use of a short, shared, secret-key, executes a simple binary decision rule on every transmitted bit. An eavesdropper, on the other hand, who does not possess the secret-key, is subjected to an irreducible quantum uncertainty in each measurement, even with the use of ideal detectors. We have implemented this scheme to demonstrate quantum-noise–protected data encryption at 650 Mbps through a 200 km, in-line amplified, WDM line. The line simultaneously carried two 10 Gbps standard data channels, 100 GHz on either side of the encrypted channel, which shows that this scheme is compatible with the widely deployed WDM fiber-optic infrastructure.

A NOTE OF THANKS

First of all, I would like to thank the organizers of this conference—Steve Barnett, John Jeffers, and other members of the organizing committee—for assembling an excellent program for the meeting and ensuring smooth and hospitable environment for all attendees. I am particularly thankful because, having organized the 4th conference of this series at Northwestern University in 1998, I know firsthand how difficult a job this can be. Having said that, I will begin this talk by expressing my heartfelt delight at being chosen to receive the 5th International Quantum Communication Award “for the contribution of challenging work on experimental quantum communication and quantum cryptography for the real world.” It is truly an honor and a source of pride to be listed among such distinguished colleagues and pioneering scientists who have been the past recipients of this award. I want to take this opportunity to thank my colleagues for nominating me and even more for selecting to bestow such an honor upon me. I also want to express my thanks to all my students, post-doctoral associates, and collaborators, past and present, for their hard work and contributions to the accomplishments that have made this recognition possible. I am also very grateful for the support of my colleagues, Horace Yuen in particular, in the Electrical and Computer Engineering and Physics and Astronomy departments at Northwestern who help create an excellent environment for success, without which such accolades would not be possible.

As the title of my presentation suggests, the overarching goal of the work that my research group has been carrying out for the last several years is to develop means to permeate quantum optical technology into real-world fiber-optic systems. To date, all such systems, although deployed on a global scale, operate in the classical domain wherein the quantum properties of light are not exploited for any potential benefit. In this presentation I summarize our recent progress towards utilizing nonclassical features of light for developing quantum communication and cryptography applications that are compatible with real-world wave-division-multiplexed (WDM) optical networks.
I present our recent results on two fronts: i) telecom-band in-fiber entanglement generation, storage, and long-distance distribution and ii) quantum-noise protected high-speed data encryption through an optically-amplified WDM line. Along the first front, using our in-fiber source of polarization-entangled photon pairs we have demonstrated that entanglement can be stored for up to 1/8 of a millisecond by propagating one photon of the pair through a 25 km spool of fiber. Additionally, when each photon of the entangled pair is propagated through separate 25 km-long spools of fiber, high visibility quantum interference is still observed, demonstrating that this system is capable of long-distance (> 50 km) entanglement distribution. Along the second front, we have implemented a new quantum cryptographic scheme, based on Yuen’s KCQ protocol, in which the inherent quantum noise of coherent states of light is used to perform the cryptographic service of data encryption. We have demonstrated quantum-noise-protected data encryption at 650 Mbps through a 200 km, in-line amplified, WDM line. The line simultaneously carried two 10 Gbps standard data channels, 100 GHz on either side of the encrypted channel, which shows that this scheme is compatible with the widely deployed WDM fiber-optic infrastructure.

TELECOM-BAND IN-FIBER ENTANGLEMENT GENERATION, STORAGE, AND DISTRIBUTION

Entangled photon-pairs are a critical resource for realizing the various quantum information processing protocols such as quantum teleportation [1, 2] and quantum cryptography [3]. Because of the requirement of distributing entangled photons over long distances and the difficulty of coupling entangled photons produced by $\chi^{(2)}$ nonlinear crystals into optical fibers [4], a source emitting entangled photon-pairs in the low-loss 1550 nm telecommunication band of silica fiber that could be directly spliced to the existing fiber network is desirable. We have recently developed such a source by exploiting the $\chi^{(3)}$ (Kerr) nonlinearity of the fiber itself [5, 6]. When the pump wavelength is close to the zero-dispersion wavelength of the fiber, phase-matching is achieved and the probability amplitude for inelastic four-photon scattering (FPS) is significantly enhanced. In this process, two pump photons at frequency $\omega_p$ scatter through the Kerr nonlinearity of the fiber to create energy-time entangled Stokes and anti-Stokes photons at frequencies $\omega_s$ and $\omega_a$, respectively, such that $2\omega_p = \omega_s + \omega_a$. Because of the isotropic nature of the Kerr nonlinearity in fused-silica-glass fiber, the scattered correlated-photons are predominantly co-polarized with the pump photons. By coherently adding two such orthogonally-polarized parametric processes, polarization entanglement has been created as well [6]. Following this approach, all four Bell states can be prepared, and a violation of Bell’s inequalities by up to 10 standard deviations of measurement uncertainty has been demonstrated [6].

Progress on Entangled Photon-Pair Generation

In early experiments with this source, the number of measured total-coincidence counts between the Stokes and anti-Stokes photons exceeded the number of accidental-coincidence counts by only a factor of 2.5 [5]. We have recently shown that spontaneous Raman scattering accompanying FPS causes this problem [7]. By reducing the detuning between the Stokes and pump photons and by using polarizers, we have demonstrated that the accidental coincidences can be made less than 10% of the true coincidences at a production rate of about $\bar{n} = 0.04$ photon-pairs/pulse [8].

Our experimental setup is shown in Fig. 1. Stokes and anti-Stokes photon-pairs at frequencies $\omega_s$ and $\omega_a$, respectively, are produced in a nonlinear-fiber Sagnac interferometer (NFSI). We have previously used this NFSI to generate quantum-correlated twin beams [9], correlated photon-pairs [5], and polarization entanglement [6]. The NFSI consists of a fused-silica 50/50 fiber coupler spliced to 300 m of dispersion-shifted fiber (DSF) with a zero-dispersion wavelength at $\lambda_0 = 1535 \pm 2$ nm. The efficiency of FPS in DSF is low because of the relatively low magnitude of the Kerr nonlinearity; only about 0.1 photon-pair is produced by a typical 5-ps-duration pump pulse that contains approximately $10^8$ photons. To reliably detect the scattered photon-pairs, a pump to photon-pair rejection ratio in excess of 100 dB is required. We achieve this by first exploiting the mirror-like property of the NFSI [10], which provides a pump rejection greater than 30 dB, and then sending the transmitted scattered photons along with the leaked pump photons through a free-space double-grating spectral filter (DGSF) that provides a pump-rejection ratio in excess of 75 dB. The filter consists of three identical diffraction gratings (holographic, 600 grooves/mm), G1, G2, G3, whose diffraction efficiencies for the horizontally and vertically polarized light are 90% and 86%, respectively. The doubly-diffracted Stokes and anti-Stokes photons are then re-coupled into fibers. The passbands for the Stokes and anti-Stokes channels
are determined by the numerical apertures of the fiber and the geometrical settings of the optical elements composing the spectral filter.

The pump is a 5-ps-duration mode-locked pulse train with a repetition rate of 75.3 MHz, obtained by spatially dispersing the output of an optical parametric oscillator (OPO) (Coherent Inc., model Mira-OPO) with a diffraction grating; its central wavelength can be tuned from 1525 to 1536 nm. To achieve the required power, the pump pulses are then amplified by an erbium-doped fiber amplifier (EDFA). Photons at the Stokes and anti-Stokes wavelengths from the OPO that leak through the spectral-dispersion optics, and from the amplified spontaneous emission (ASE) from the EDFA, are suppressed by passing the pump through a 1nm-bandwidth tunable filter (Newport, model TBF-1550-1.0). For alignment purposes, weak signal pulses at the Stokes wavelength, which are temporally synchronized with the pump In, are used to temporally synchronize the pump pulses, are injected into the EDFA. During photon counting measurements, however, the input signal is blocked.

Photon counters consisting of InGaAs/InP avalanche photodiodes (APD, Epitaxx, model EPM 239BA) operated in a gated-Geiger mode are used to count the Stokes and anti-Stokes photons [5]. The 1-ns-wide gate pulses arrive at a rate of 588 kHz, which is 1/128 of the repetition rate of the pump pulses. The quantum efficiency for one detector is 25%, that for the other is 20%. The total detection efficiencies for the Stokes and anti-Stokes photons are about 8% and 6%, respectively, when the efficiencies of the NFSI (82%), 90/10 coupler, double grating filter (45% and 50% in anti-Stokes and Stokes channel, respectively), and other transmission components (about 90%) are included.

For the FPS occurring in the DSF, the scattered correlated photon-pairs are predominantly co-polarized with the pump photons. A polarization beam splitter (PBS) is placed in both the Stokes and anti-Stokes channels. With proper settings of the half-wave-plate (HWP) and the quarter-wave-plate (QWP), which are placed in front of the double grating filter, the Stokes and anti-Stokes photons that are either co-polarized or cross-polarized with the pump photons can be rejected. We measure the number of scattered photons per pump pulse, co-polarized and cross-polarized with the pump, respectively, that are detected in the anti-Stokes channel, $N_a$, as a function of the number of pump photons per pulse, $N_p$, and the coincidence rate between the detected Stokes and anti-Stokes photons as a function of $N_a$. In both co- and cross-polarized cases, we fit the measured data with $N_a = s_1 N_p + s_2 N_p^2$, where $s_1$ and $s_2$ are the linear and quadratic scattering coefficients, respectively. Figure 2 shows the data obtained when the detuning $\Omega/2\pi$ of the Stokes (anti-Stokes) photons is 0.5 THz, where $\Omega = \omega_a - \omega_s = \omega_a - \omega_p$, and the full-width at half maximum (FWHM) of the DGSF is 0.8 nm. As shown in the inset of Fig. 2(a), for the photons co-polarized with the pump, the quadratic scattering owing to FPS dominates over the linear scattering. The main body of Fig. 2(a) shows that the total-coincidence rate of the Stokes and anti-Stokes photons produced by the same pump pulse is much higher than the accidental-coincidence rate. The latter is obtained by measuring the coincidence rate between the Stokes and anti-Stokes photons produced by two adjacent pump pulses and fits the theory curve for two independent light sources very well [5]. Comparing the coincidence-measurement results in Fig. 2(a) with our previous results in [5], the ratio between the total coincidences and the accidental coincidences is improved. Taking into account the total detection efficiency of 6% in the anti-Stokes channel, at the production rate of about $\pi = 0.04$ photon-pairs/pulse, the ratio between the total coincidences and the accidental coincidences is 13.

The results for the photons cross-polarized with the pump are shown in Fig. 2(b), where we find no difference between the total-coincidence rate and the accidental-coincidence rate. The linearly-scattered photons contribute much more than the quadratically-scattered photons, as shown in the inset of Fig. 2(b). Absence of true coincidences, which is quantified by the difference between the total-coincidence rate and the accidental-coincidence rate, implies that

---

**FIGURE 1.** Experimental setup: scattered Stokes and anti-Stokes photons emerging from the port labelled “Out” are detected; FPC, fiber polarization controller; PBS, polarization beam splitter; G, grating; QWP, quarter-wave plate; HWF, half-wave plate.
To demonstrate the practicality of our fiber-based source of polarization-entangled photons [6] in long-distance distribution of entanglement, we separated the Stokes and anti-Stokes photons, which are entangled in polarization but have different wavelengths, from each other by use of an optical filter and launched them into separate 25-km-long spools of standard single-mode fibers, as schematically shown in Fig. 3(left). The spools of fiber are commercially available; the fiber in one spool is Corning SMF-28 and that in the other is Corning LEAF. The propagation loss through each spool of fiber was measured to be approximately 0.2dB/km. Fiber polarization controllers were spliced into the photon propagation path at the end of each spool of fiber and test pulses of known polarization states were used to align the polarization axes (horizontal and vertical) at the input and output ends of the two fibers. A polarizer was used at the output end of each fiber to project the polarization state of the emerging photon to 45° vertical.

After 25 km of propagation in separate spools of fiber, the emerging Stokes and anti-Stokes photons were detected in coincidence. Appropriate delays in the photon-counting electronics were introduced to account for the propagation time in the two fiber paths. Two-photon interference experiments were conducted by detecting the emerging Stokes and anti-Stokes photons in coincidence as a function of the relative phase \( \phi_p \) between the two pump pulses that create the polarization entanglement in the source, which is 25 km away from each detector. The results are shown...
in Fig. 3(right), where no interference is observed in the single counts whereas high-visibility (86%) interference is observed in the coincidence counts. These results clearly show that high-fidelity polarization entanglement can survive even when each photon of the entangled pair has propagated through a separate spool of 25-km-long fiber and that entanglement distribution over 50 km is possible.

In order to demonstrate that a spool of fiber can be used as a quantum-memory element, we launched one photon of the entangled pair into the 25 km spool of fiber, while detecting the other without such propagation, as schematically shown in Fig. 4(left). As in the entanglement distribution experiment described above, polarization controllers and test pulses of known polarization states were used to align the polarization axes (horizontal and vertical) at the input and output ends of the fiber. Before detection, the polarization state of both the photons was projected at 45° relative to the vertical. In this case, an appropriately long delay in the photon-counting electronics was introduced to account for the propagation time (0.125 ms) of the photon through the 25 km of fiber. Once again, two-photon interference experiments were conducted by detecting the emerging Stokes and anti-Stokes photons in coincidence as a function of the relative phase \( \phi_p \) between the two pump pulses that create the polarization entanglement in the source. The results are shown in Fig. 4(right), where no interference is observed in the single counts whereas high-visibility (80%) interference is observed in the coincidence counts. These results clearly show that high-fidelity polarization entanglement can survive even when one photon of the entangled pair is detected immediately, while the other is held for 1/8 ms in a spool of fiber. In other words, a spool of fiber can indeed serve as a high-fidelity quantum memory element.
QUANTUM-NOISE PROTECTED HIGH-SPEED DATA ENCRYPTION

For more than twenty years, physicists and engineers have investigated quantum-mechanical phenomena as mechanisms to satisfy certain cryptographic objectives. Such objectives include user authentication, bit commitment, key generation, and, recently, data encryption. To date, the cryptographic objective most considered in the literature has been key generation. In key generation, two users, who initially share a small amount of secret information, remotely agree on a sequence of bits that is both larger than their original shared information, and known only to them. The newly generated bits (keys) are then used to publicly communicate secret messages over classical channels by driving data encrypters like the information-theoretically secure one-time pad (OTP) [11] or more efficient (but less secure) encrypters, such as the Advanced Encryption Standard (AES), deriving their security from complexity assumptions [12, 13].

Several approaches to key generation using quantum effects have been proposed and demonstrated. The most famous of these protocols, the BB84 protocol [14] and the Ekert protocol [15] have enjoyed considerable theoretical consideration as well as experimental implementation [16, 17, 18]. A major technical limitation of the BB84 (Ekert) protocol is that the achievable key-generation rate (more importantly, the rate-distance product) is relatively low due to the protocol’s requirement for single-photon (entangled-photon) quantum states. This requirement is a burden not only in the generation of such states, but also in that such states are acutely susceptible to loss, are not optically amplifiable (in general), and are difficult to detect at high rates. Furthermore, because the received light must be detected at the single-photon level, integration of the protocol implementations into today’s wavelength-division-multiplexed (WDM) fiber-optic infrastructure is problematic because cross-channel isolation is typically no better than 30dB.

Recently, we have demonstrated a new quantum cryptographic scheme, based on Yuen’s KCQ protocols [19], in which the inherent quantum noise of coherent states of light is used to perform the cryptographic service of data encryption [20, 21]. Unlike single-photon states, coherent states (of moderate energy level) are easily generated, easily detected, and are optically amplifiable, networkable, and loss tolerant. Note that key generation and data encryption are two different cryptographic objectives with different sets of criteria by which to judge performance—a direct comparison between the two cannot be made trivially.

In our scheme a legitimate receiver, with use of a short, shared, secret-key, executes a simple binary decision rule on every transmitted bit. An eavesdropper, on the other hand, who does not possess the secret-key, is subject to an irreducible quantum uncertainty in each measurement, even with the use of ideal detectors. Our scheme, running at data-encryption rates up to 650Mbps, uses off-the-shelf components and is compatible with today’s optical telecommunications infrastructure. Below we summarize our recent experimental results applicable to wave-division-multiplexed (WDM) optical networks.

**Time-Mode Implementation**

The requirement of polarization-state alignment at the receiver by the polarization-mode scheme that we previously implemented [21] makes it much less attractive for deployment in real WDM optical networks. We have recently implemented a time-mode version of the protocol that is polarization-insensitive with equivalent performance [22, 23]. This implementation is totally polarization-state insensitive and is, therefore, much more desirable for performing quantum-noise-protected data encryption over real-world WDM networks.

A description of the time-mode experimental setup naturally breaks into two parts: the transmitter/receiver pair and the WDM fiber line. We first describe the transmitter/receiver pair. As illustrated in Fig. 5(left), −25dBm of power from a 1550.9nm-wavelength DFB laser is projected into Alice’s 10GHz-bandwidth fiber-coupled PM. Driven by the amplified output of a 12-bit D-A board, the modulator introduces a relative phase (0 to $2\pi$ radians) between temporally neighboring symbols. A 4.4-kb software LFSR, which is implemented on a PC, yields a running-key that, when combined with the data bit, instructs the generation of one of two coherent states required by the protocol at 650Mbps data rate [23]. Before leaving the transmitter, the encrypted signal is amplified with an EDFA (OA1) to a saturated output power of 2dBm.

On passing through the 200km-long WDM line [shown in Fig. 5(right), Crypto. in and Crypto. out], the received light is amplified by another EDFA (OA2) with $\approx$ 30dB of small-signal gain and a noise figure very close to the quantum limit (NF $\approx$ 3dB). The light then passes through a pair of 10GHz-bandwidth polarization-maintaining-fiber-coupled PMs oriented orthogonally with respect to each other so that the $\hat{x}$ ($\hat{y}$) polarization mode of the first modulator projects onto the $\hat{y}$ ($\hat{x}$) mode of the second modulator. The effect of such concatenation is to apply an optical phase
modulation that is independent of the polarization state of the incoming light. The relative phase shift introduced by Bob’s modulator pair is determined by the running-key $R$ generated through a software LFSR in Bob’s PC and applied via the amplified output of a second D-A board. After this phase shift has been applied, the relative phase between temporally neighboring states is 0 or $\pi$ (differential phase-shift keying), differentially corresponding to a 0 or 1.

The decrypted signal then passes through a fiber-coupled optical circulator and into a temporally asymmetric Michelson interferometer with one bit-period round-trip path-length delay between the two arms. Use of Faraday mirrors (FM) in the Michelson interferometer ensures good polarization-state overlap at the output, yielding high visibility interference. The interferometer is path length stabilized with a PZT and dither-lock circuit.

Light from the two outputs of the interferometer is direct-detected by using two room temperature 1GHz-bandwidth InGaAs PIN photodiodes set up in a difference photocurrent configuration. The resulting photocurrent is either sampled by an A-D board and stored for analysis, or put onto a communications signal analyzer (CSA) to observe eye patterns.

As shown in Fig. 5(right), the 200km-long WDM line consists of two 100GHz-spacing AWGs, two 100km spools of single-mode fiber (Corning, SMF-28) and an in-line EDFA with an input isolator. Along with the quantum-noise protected 650Mbps encrypted-data channel, two 10Gbps channels of classical data traffic also propagate through the first 100km of the described WDM line. Light from two DFB lasers with wavelengths on the 100GHz ITU grid (1550.1nm and 1551.7nm) is mixed on a 3dB coupler, where one output is terminated and the other enters a 10GHz-bandwidth fiber-coupled Mach-Zender type LiNbO$_3$ intensity modulator (IM). The IM is driven by an amplified 10Gbps PRBS generator by a bit-error-rate tester (BERT) of $2^{31}$−1 period. The PRBS-modulated channels (hereafter referred to as PRBS channels) then pass through an EDFA to compensate for losses before entering and being spectrally separated by AWG1. Partial decorrelation of the PRBS channels is achieved by introducing approximately one meter fiber length difference ($\approx$ 50 bits) between the channels before combining them into the WDM line with AWG2. On launch (i.e., after AWG2), the optical power is $-2$dBm/channel for all three channels.

After propagating through the first 100km of fiber (20dB of loss) and the in-line EDFA (23dB of gain), the channels are separated by AWG3 (3dB of loss). Either of the two PRBS channels is amplified with a 10dB gain EDFA and the GVD is partially compensated by a $-1530$ps/nm DCM. The amplified, GVD-compensated PRBS channel is detected using an InGaAs PIN-TIA receiver (RCVR) and analyzed for errors by the BERT. Note that the reason that the PRBS channels do not propagate through the entire 200km line is because our DCM only provides enough compensation for 100km of fiber. The bit-error rate for each of the PRBS channels remained nearly “error free” at $5 \times 10^{-11}$ despite the incomplete GVD compensation.

Figure 6 shows the eye patterns for encrypted 650Mbps ($2^{15}$ − 1)-bit-PRBS and 1Mb-bitmap-file transmissions (insets) as measured by Bob (left) and Eve (right). In these experiments, Bob is located at the end of the 200km-long line and Eve is located at the transmitter (Alice). Eve’s actions are physically simulated by using Bob’s hardware, but starting with an incorrect secret-key. While Fig. 6(right) does not explicitly demonstrate Eve’s inability to distinguish neighboring coherent states on the phase circle, it does, however, show that a simple bit decision is impossible. The Q-factor for Bob’s eye pattern, as measured on the CSA, was 12.3.

In all of the time-mode implementation experiments, the coherent states are transmitted using non-return-to-zero (NRZ) format. The return-to-zero-like appearance of Bob’s eye pattern is due to non-zero rise time of the optical
phase modulation. This phenomena is also observed in traditional NRZ-DPSK systems. The apparent banding of Eve’s measurements at the top and bottom of the eye pattern is due to the sinusoidal transfer function of the temporally asymmetric interferometer used for demodulation. Despite this apparent banding, the eavesdropper’s probability of error is equal for every transmitted bit. If an eavesdropper were to, say, perform optical heterodyne detection, a uniform distribution of phases would be observed.

In the current setup, the 12-bit D-A conversion allows Alice to generate and transmit 4094 distinct phase states ($M = 2047$ bases). Although we simulate an eavesdropper by placing Bob’s equipment at the transmitter, a real eavesdropper would aim to make the best measurements allowed by quantum mechanics. Our numerical calculations show that for $-25$dBm signal power at 650Mbps ($≈ 40,000$ photons/bit) with $M = 2047$, Eve’s maximum obtainable information in an individual attack on the message would be less than $10^{-15}$ bits/bit.

ACKNOWLEDGMENTS

I would like to sincerely thanks all my students, postdocs, and collaborators, past and present, for their hard work, without which the accomplishments presented here would not be possible. The research presented here has principally been carried out by Dr. Xiaoying Li, Dr. Paul Voss, Jun Chen, Sarah Dugan, Eric Corndorf, Chuang Liang, Dr. Greg Kanter, Dr. Vladimir Grigoryan, Dr. Marco Fiorentino, and Dr. Jay Sharping. Last, but not the least, I wish to thank the sponsors of this work. The work on fiber-based entanglement generation and distribution is funded through a DoD Multidisciplinary University Research Initiative (MURI) Program under a U.S. Army Research Office collaborative Grant (DAAD19-00-0177) to Massachusetts Institute of Technology and Northwestern University. I am indebted to Dr. Henry Everitt of the ARO for making this grant possible. The work on quantum-noise protected data encryption has been made possible by the U.S. Defense Advanced Research Projects Agency under Grant F30602-01-2-0528. I am greatly appreciative of the generous support that Dr. Mike Foster of DARPA has given to this project.

REFERENCES


