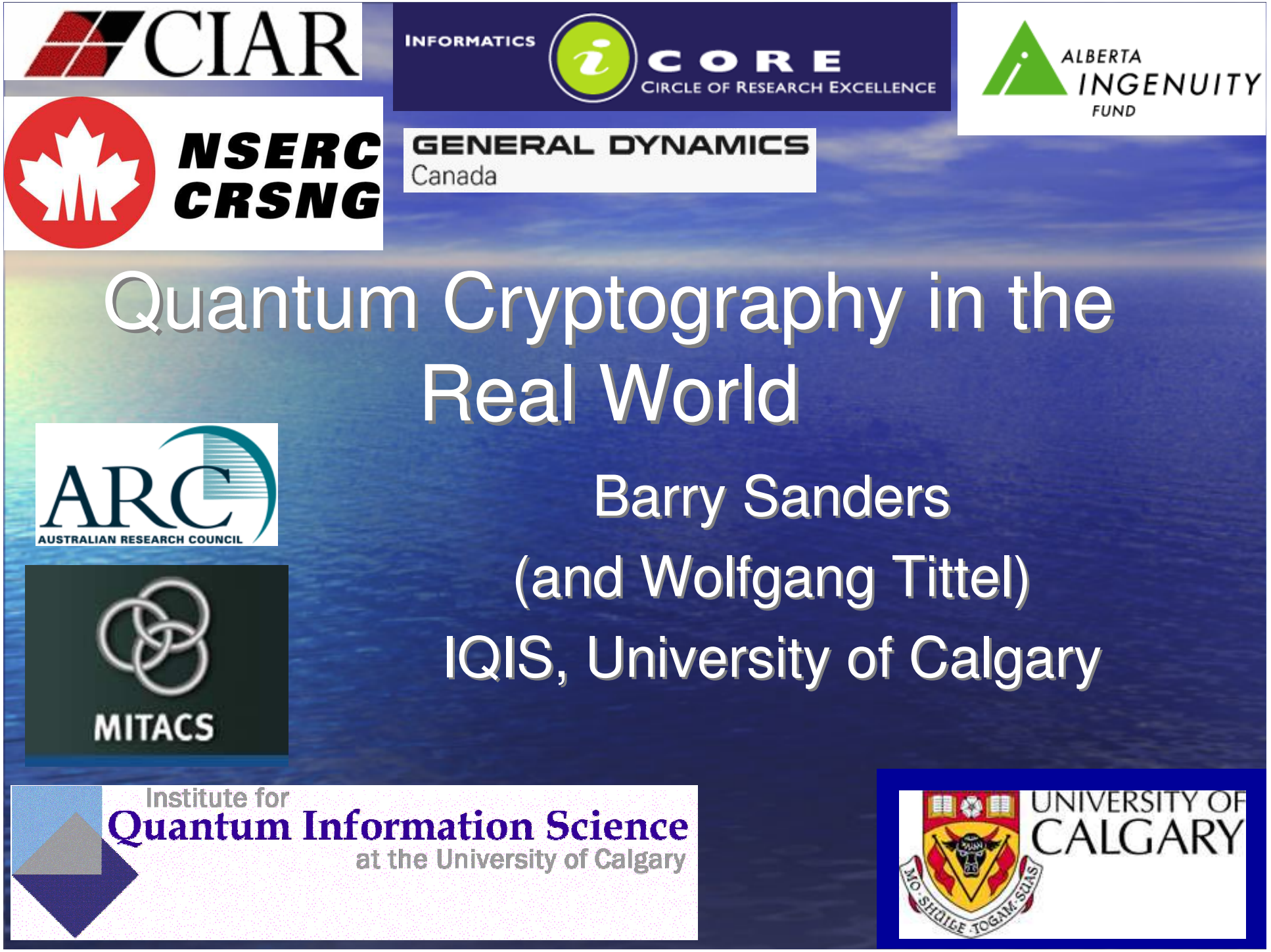
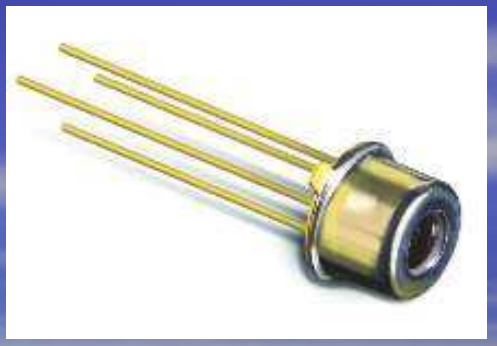

CIAR
INFORMATICS
iCORE
CIRCLE OF RESEARCH EXCELLENCE
ALBERTA INGENUITY FUND
NSERC
CRSNG
GENERAL DYNAMICS
Canada
Quantum Cryptography in the Real World
ARC
AUSTRALIAN RESEARCH COUNCIL
Barry Sanders
(and Wolfgang Tittel)
IQIS, University of Calgary
MITACS
Institute for
Quantum Information Science
at the University of Calgary
UNIVERSITY OF CALGARY
MO · SHUILE · TOGAM · SUMS

- Goal: 10 Mbit/s (10 MHz) secret key generation rate, for a one-time pad or more likely with AES. For 256 bit AES, refresh rate is ~40/ms.
- Current typical rate: 10 kHz using 2 MHz clock rate pulse generation over 10 km with $\langle n \rangle$ per pulse of 0.2.
- Slow clock because InGaAs avalanche photo detector (APD) rate cannot exceed ~MHz because of dead time.
- 10 GHz clock suffices for 10 Mbit/s.

Why is APD so slow?



- Weak field sensitivity requires large gain G for small change in detector voltage V.
- InGaAs APD features flat G vs V until breakthrough V (BV): sudden jump to ∞.
- Bias APD just below BV then clock triggers V above BV for 2ns to detect: short window hence low dark count rate p_D.
- Can't gate faster than 2 MHz because electrons trapped in impurities must be released or else we obtain after-pulses: this dead time of 1 μs limits clock speed to MHz.

Quantum efficiency and dark counts for InGaAs APD

- Quantum efficiency (QE) is probability of detection given a photon is sent: QE~0.1.
- Dark count rate p_D is probability of photo detection when none sent: $r \sim 10^{-5}$ in 2 ns.
- Above BV, QE ↑ with V but p_D ↑ faster.
- Quantum bit error rate (QBER) is error probability given signal photon and is a function of *r* and arrival probability.
- Detector is critical: clock rate, QE, and p_D.

Photon number splitting (PNS) attack

- PNS reads qubit by peeling photons from multiphoton pulses so pulses must be weak.
- Alternative: decoy states achieve 0.5 photon per pulse (but what about for quantum repeaters?).
- Post-processing: error correction, privacy amplification, authentication performed by software, but may not be fast enough for GHz clock rates - will need hardwired chips.

Fast clock vs short pulses

- We want 10 GHz clock for pulses.
- Inter-pulse spacing of 100 ps implies pulses need to be shorter than 50 ps hence rapid switching to each of the four BB84 states.
- Require detectors with dead times << 1 μs.
- Need excellent clock synchronization for Alice to know which pulse arrived.

Active stabilization of quantum channel

- Polarization decoheres due to time-varying birefringence.
- Avoid polarization decoherence via time-bin encoding but requires phase-locking between Alice's and Bob's interferometers.

Complicated networks

- Hybrid quantum channels: need to convert between fibre and free space channels for satellite etc communication.
- Topologies for multiple users, e.g. star.
- Synchronization is a challenge.

Beating distance barriers

- Point-to-point protocols (requires trust).
- Quantum relays (e^{-L}) via teleportation, entanglement swapping, and quantum error correction to correct for noisy detectors etc but not yet for decoherence in fibre as this is negligible: allows infinite distance but at exponentially small rates.
- Quantum repeater: poly(distance).
- Quantum memory required for relay and for repeater.

Relay

- Uses entanglement swapping and linear optics.
- Works maximum 50% of the time.
- Timing is critical: photon pair must arrive simultaneously (relative to coherence time and, although coherence length is 1 μm, heating is a problem: 1 km fibre heating 1˚ extends 8 mm) at the beam splitter which projects to Bell state.
- Improve coherence either by active stabilization or by spectral filtering to increase coherence time, but this reduces rate of entangled photon pairs within filtered bandwidth.

Next generation of detectors

- Transition-edge sensor (TES): QE~0.9, p_D ~1/day (but requires enormous spectral filtering to eliminate infrared and other counts).
- Although QE and p_D are good, the TES is slow so clock speed limited to kHz.

Inefficient key distribution

- Photon pairs now are probabilistic based on spontaneous parametric down conversion.
- Detectors are effectively probabilistic, i.e. inefficient (10% at telecom wavelength).
- Transmission is probabilistic (loss rate of 0.2 dB per km at telecom wavelength).
- If we can make pairs on demand (e.g. using quantum dot sources) and improve QE, then quantum cryptography based on entanglement obviates decoy state requirement.

Quantum memory

- Preserve quantum information in cooled ions within crystals or fibres.
- Crystals can have embedded waveguides.
- Ions are cooled cryogenically.
- Each rare earth ion can be a two- or three-level atom with narrow homogeneous line width but significant inhomogeneous broadening due to crystal defects and lattice strain.
- Use photon echoes to store quantum information: “rotate” ion state where it diffuses, then flip to cancel diffusion and “rotate” back.

Apply photon echo to memory

- Medium is prepared in the state where the inhomogeneous broadening is controllable by electric field: photon is absorbed so photon bandwidth must match medium bandwidth ~ 200 MHz for nanosecond pulses.
- Store photon and switch off the electric field.
- Retrieve photon by turning on electric field.
- Storage time at least 500 μs/km but is less than coherence time.

Problem with multiple photons in relay

- Alice prepares state with multiphoton component and uses decoy state but then the probability of getting false BSM from both photons being from source is a problem and this leads to error rate. Need to weaken decoy state but this may be at expense of high error rate.
- Second thing is how can eavesdropper take advantage of the use of decoy states in relay and how to protect against this.

Of course: commercial issues

- Integration and packaging.
- Ease of operation (user friendly).
- Limit ageing of system and devices.
- Test bed for these issues.

Main points

- Goal is MHz key generation from current kHz rates.
- The next breakthroughs require new detectors: TES is slow but is efficient and has low dark count rate, but will require new detector technology with time jitter ~10 ps.
- Need pulses ~50 ps with inter-pulse separation ~100 ps; on-demand preferred.
- Quantum memory will be needed for synchronization: photon transit time over 100 km is ~500 microseconds to memory should be at least 10 ms, which allows collection of data from all memory points to travel back and forth to send instructions to memories for several hundred km).

Photon echo

- Now apply electric field to shift absorption line or split line in 3LA: important thing is that some atoms will shift to positive frequency by some amounts and others to negative frequency by some amounts so now there is inhomogeneously broadened medium but due to controllable applied electric field. Now absorb light and reverse absorption (storage) process so light should be re-emitted in reverse direction, and this requires two steps: reverse gradient (negative to positive voltage) to undo dephasing, then need position-dependent phase shift so go in with e^{ikz-iwt} and in reverse direction z --> -z then can show that these two conditions lead to time reversal of absorption process as long as all decoherence effects are smaller than storage time.

To use photon echo

- Use three-level version with applied electric field controlling inhomogeneous broadening.
- Need right medium with huge absorption depth and sufficiently long coherence time (fibre is great for absorption depth but bad for coherence time which is microseconds at best).
- Alternative: crystalline waveguides which have millisecond coherence time.
- Have to worry about optical pumping, controlled reversible broadening, and position-dependent phase shift.
- Qubits arrive at GHz rate and want to store