Quantum Communications and Quantum Computing for C4I

Ronald E. Meyers and Keith S. Deacon
Army Research Laboratory
Adelphi, Maryland 20783

Abstract

Advances in science and technology and CISD ARL's quantum computing simulations and research support the conclusions that a concerted effort, could for the Army's Objective Force, a) initiate implementation of ultra-secure stealth Quantum communications and quantum imaging now, and b) implement within 5 years Type II Quantum Computing with its much greater than classical computing power to solve key IT/C4ISR problems.

1. Introduction

The mission of our Quantum Communications and Quantum Computing Team in the Computational and Information Sciences Directorate (CISD) at the Army Research Laboratory (ARL) is to conduct basic and applied research into quantum computing and quantum communications. This follows the direction of the Quadrennial Defense Review of 30 September 2001 " The Department [of Defense] will vigorously pursue…technologies that can significantly increase U.S. advantage in intelligence collection, analysis, and security. Some of the promising include: …quantum computing to provide real-time processes, decryption, translation, and transcription of communications."

2. Quantum Communications for the Objective Force

The bandwidth and speed challenges to military communications and computing are led by the constraints of security, survivability and deployability. Quantum communications can be more secure than conventional military communications because it employs quantum physics properties, which allow the detection of any eavesdropper. Quantum states cannot be instantaneously cloned. An increase in error rates in the exchange of quantum keys between sender and receiver warns of an eavesdropper. Conventional military communications cannot detect eavesdroppers. C4I for the Objective Force could take advantage of advanced quantum communications capabilities to improve its security. Recent advances in quantum communications theory, numerical simulation, and experiments in our laboratory and elsewhere demonstrate the potential of employing entangled photon technology for quantum communications for the Objective Force. Quantum communications would provide the Objective Force a decisive security advantage on the future battlefield.

2.1 Quantum Communications in CISD ARL

We have developed and are testing in our laboratory two entangled photon quantum communication systems (See Fig 1.), and have analyzed the use of laser array systems for quantum use (Meyers, Deacon, et. al., 2002b). These systems prove that entangled photons can provide both free-space and fiber optic secure shared quantum keys. Eavesdroppers can be detected by monitoring the error rates. The distributed shared cryptographic quantum keys can be used for many purposes. Battlefield quantum keys could be distributed through satellites. An important use would be for satellite cryptographic device re-keying. Battlefield cryptographic keys could be generated by quantum means and then distributed by classical channels. Later all quantum channels would be utilized. We recommend an R &D quantum computing reach-back facility at CISD ARL to tie into the Objective Force and emerging implementations such as the Quantum Internet, and battlefield Robots, RPVs, and MAV's.

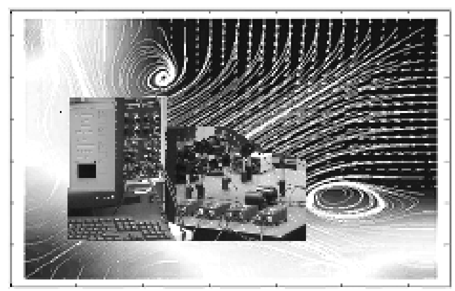

Fig. 1 ARL CISD Quantum Entangled Photon Shared Quantum Key Distribution System viewed against a backdrop Simulation of Type II Quantum Computing Solution of NSE Fluid Flow.

3. Quantum Computing for the Objective Force

Quantum computing will probably see it's first implementation in military settings in the form of devices solving special problems rather than general-purpose quantum computers. This emulates the initial defense use of classical computers. Quantum imaging, quantum communications, quantum clock synchronization, and other quantum technologies may be implemented to process information in non-classical ways in place of classical computing as part of a quantum information processing or quantum computing environment. Just as the PC and the Internet are connected, quantum computing and quantum communications (and other quantum technologies) will be inexorably connected to do work the Army's Objective Force needs. Quantum imaging and quantum communications can be implemented now, and the future for IT/C4ISR quantum computing can be planned now.

3.1 Type II Quantum Computing

A quantum computer is a very exciting prospect since unlike classical computers it maintains a quantum mechanical superposition of states. This gives it exponential computing capacity. Most research has gone toward the development of universal quantum computers. A universal quantum computer must be able to perform several types of operations. These include the challenging C-not operation. But Universal quantum computers have several drawbacks also. a) First, they do not utilize all of quantum physics, leaving out quantum analog computing which exploits the direct mapping of quantum physics to problems. b) The second drawback of the universal quantum computer is that it may not be optimal for solving a particular problem of interest. c) The third drawback is that it will take longer to develop a universal quantum computer capable of solving Shor's algorithm for large prime factorization, than it will take to design and manufacture quantum computers for solving specific important military and public applications.

A Type II Quantum Computing capability is possible for the Army's Objective force within five years if a concerted effort is put forth in that direction. A Type II Quantum computer has arrays of quantum nodes; each node with a few qubit capability, and each node is coupled with classical communication to nearby nodes. We can show that a Type II quantum computer array could become more powerful than the classical computing capability for solving many problems important for the Army. Several technologies for making few qubits per quantum node computers are possible now. Photon quantum computers have been demonstrated, as have NMR quantum computers at low qubit numbers. We have designed our own version of a Type II quantum computer to solve fluid dynamics problems, although we have not implemented it yet. We have also recently designed a photon C-Not gate for the universal type of quantum computer. Technologies are being developed which show promise toward making Type II quantum computer node arrays available for solving important Army problems using techniques we have simulated in Figs. 1 and 2.

3.2 Quantum Computing Simulations in CISD ARL

We have developed quantum software to simulate Type II Quantum Computers solving key problems of interest to the Army and some results are shown in Figs. 1 and 2. In particular we have developed one, two, and three dimensional quantum computing partial differential equation solvers simulating fluid dynamics problems confronting the Army. These are based on the mathematics developed simulating the evolution of the quantum wavefunction, the quantum probability density function, and the Navier Stokes Eqs. (Meyers, Deacon, Rosen 2002; Zak, Zbilut, Meyers, 1997;Yepez, 2001). Simulated Quantum computing test problems solved include a) compressible turbulent air and sound wave dynamic gas flow interacting with a helicopter, b) turbulent airflow through a person's respiratory tract, and c) turbulent compressible NSE airflow around complex objects.

In addition, our analysis shows that quantum computing can be applied to solving such battlefield problems as recognizing tanks and airplane images from other images. Quantum simulations of such complex problems as decision-making and intelligence analysis are possible with Type II and related Quantum recurrent computers (Zak, Meyers, Deacon, 2000).

Fig. 2 ARL CISD Simulation of Type II Quantum Computing Solution of NSE Flow Around a 2D model of an Army Helicopter.

Conclusion

The Army's Objective Force could benefit from implementing quantum communications, quantum imaging and Type II quantum computing, if sufficient effort is put into it, within a period of five years.

References

Meyers, R. E., K. S. Deacon, D. L. Rosen, "Numerical Simulation of Linear and Nonlinear Quantum Optics as a Design Tool for Quantum Communications," SPIE, Jul 2002

Meyers, R. E., K. S. Deacon, et. al., "Synchronized Laser Array as a Source for Quantum Communications," SPIE, Jul 2002

Zak, M., R. E. Meyers, K. Deacon, "Quantum Decision Maker: Theory and Simulation", SPIE, Apr 2000

Zak, M., J. Zbilut, R.E. Meyers, *From Instability To Intelligence*, Springer Verlag, 1997, 550p

Yepez, J., "Type II Quantum Computers", *Int. J. Mod. Phys. C*, Vol. 12, No. 9, p1273-p1284, Nov. 2001.