A MITACS Business Plan for a Consortium

November 15, 2001

1 Title of Project

Quantum Information Processing

2 Purpose

3 Project Members

4 Industrial Affiliates

5 Project Description and Methodology

5.1 Quantum Algorithms and Complexity Theory

5.2 Quantum Circuit Complexity

5.3 Communication Complexity

5.4 Quantum Information Security

This part of the proposal addresses the impact of quantum computation and quantum communication on the field of cryptology. We can break this up into three parts.

SINCE I DIDN'T KNOW HOW YOU USE REFERENCES, I DID NOT MAKE ANY SPECIFIC *cite* ANYWHERE. YOU ARE WELCOME TO FIX THAT. IS THIS TEXT WAY TOOL LONG ??

5.4.1 Cryptography for quantum data

Starting from the notion of Quantum Teleportation (due to Bennett, Brassard, Crépeau, Jozsa, Peres, Wootters), which can be viewed as the quantum equivalent of the classical one-time-pad with quantum secret keys (one-time-quantum pad) recent research has naturally

led to the notion of Quantum one-time pad that uses only a classical secret key to do perfect encryption of quantum states.

A natural extension to this concept is the notion of Public-Key Quantum Cryptography (Crépeau) which uses a classical Public-key Crypto-system to transmit the secret-key of a Quantum One-Time-Pad. Similarly the notion of Quantum Authentication has recently emerged (Barnum, Crépeau, Gottesman, Smith, Tapp) as the quantum analog with classical secret keys of the classical notion of authentication codes to protect the integrity of Quantum data. Surprisingly, although it is trivial to extend Quantum One-time-pad to Public-Key Quantum Cryptography, Quantum Digital Signatures are shown to be impossible!

But cryptography has more to offer than encryption and authentication. Other important notions such as Quantum Secret Sharing (Cleve, Gottesman, Lo, reference 2 of Cleve) and Verifiable Quantum Secret Sharing (Crépeau, Gottesman, Smith) have been introduced to allow a party to share a quantum state among several parties in such a way that a small number of them have no information about the original state, whereas sufficiently many of them can reconstruct the state accurately. It is verifiable if honest parties can check ahead of time whether the reconstruction process will work despite the presence of a few dishonest participants. The notion of Fault-Tolerant Quantum computation (Aharonov, Ben-Or), combined with Verifiable Quantum Secret Sharing, leads naturally to the development of Multiparty Quantum Computations (Crépeau, Gottesman, Smith) where several distrustful parties accomplish a quantum computation on data that they keep secret from each other. At this time the best VQSS tolerates $n/4$ out of n cheaters (this is optimal) whereas only $n/6$ cheaters can be tolerated for multiparty Quantum Computations. The gap between $n/6$ and $n/4$ remains to be investigated in future work. Moreover, the proofs of security of these protocols are not composable: given prior knowledge about earlier such protocols, the proof of security no longer works.

Other foundamental primitives such as Oblivious Quantum Transfer and Qubit Commitment (Crépeau, Dumais, Marcil) have to be investigated in relation to their classical counterparts. Combining the notion of Zero-Knowledge with Qubit Commitments is a non-trivial task that has been somewhat studied. This research is at a very preliminary stage since even a good definition of Zero-knowledge is not currently known for classical data handled by parties equipped with quantum computers.

5.4.2 Quantum Computational Assumptions and Cryptographic Primitives

Since Shor introduced his quantum algorithm for factoring large integers and extracting discrete logarithms, most computational assumptions used in modern cryptography are threatened by the development of a quantum computer. It has become a necessity to investigate new computational assumptions that could be used to do cryptography. New candidates for one-way Functions and Trapdoor One-way Functions are being considered so that they would resist Quantum cryptanalysis. Some one-way functions of McEliece and of Fischer-Stern based on coding theory problems and a one-way function of Buchmann based on number fields are relevant candidates currently under investigation. These problems are

analyzed to determine whether quantum algorithms could solve them efficiently.

Last summer, a team of researcher (Crépeau, Dumais, Mayers, Salvail) has gathered at McGill to investigate the idea of (quantum) computational assumptions in classical cryptography. We know that unconditionally hiding (and quantum-computationally binding) bit commitments can be based upon the assumption that quantum one-way permutations exist (Dumais,Mayers,Salvail). A similar result was developed for any one-way function (Crépeau, Légaré, Salvail) but at much higher cost.

The next step is to prove other protocols secure upon similar assumptions, notably the "oblivious transfer" protocol (reference [Cr94] Crépeau) based on quantum transmission. This result is believed to be false in a classical setting (one-way functions/permutations are believed to be insufficient to implement secure Oblivious Transfer).

A new primitive in quantum cryptography promises to be a useful tool in security proofs: "quantum measure commitment", the fact that a party in a protocol is committed to having measured a given quantum state. We (Crépeau, Dumais, Mayers, Salvail) have shown that quantum measure commitment can be based upon computational assumptions in some limited and ideal cases. The coherent and "imperfect" cases are still to be proven and this will be the subject of further work and discussions in a near future. Ultimately, we hope to prove security of any classical two-party Computation based on such a quantum-computational oblivious transfer.

5.4.3 Quantum Zero-Knowledge

At the border of complexity theory and cryptography are the notions of Interactive Proofs and Zero-Knowledge. These are ways for a prover to demonstrate the validity of a statement to a less powerful (or knowledgeable) verifier, in a way that does not increase the knowledge of the verifier with respect to proving such statements by himself later. Brassard and Crépeau are pioneers of this field in the classical world. Recently very interesting contributions Watrous (reference 1 of Watrous) showed that interactive proofs in the quantum world are more powerful than in the classical world, in at least two different ways: the complexity class PSPACE is included in a "bounded round" Quantum Interactive Proof class, a statement believed to be false classically, and a problem not known to be in the probabilistic complexity class MA was shown to be in its quantum analog.

Can John fill this in with his recent result on HONEST VERIFIER ZK?

New approaches have to be explored because the classical definition (through a simulator) does not extend well to the quantum scenario. The problem lies with the "auxilliary input" definition of zero-knowledge which is used to prove zero-knowledgeness of composed ZK proofs. Recent ideas (Crépeau) suggest a new definition where auxilliary inputs are useless (using proper randomization of the statement being proved) and thus might lead to a valid quantum scenario definition. This research is ongoing.