Abstract Submitted
for the MAR12 Meeting of
The American Physical Society

Universal Blind Quantum Computation JOSEPH FITZSIMONS, National University of Singapore, ELHAM KASHEFI, University of Edinburgh — Blind Quantum Computing (BQC) allows a client to have a server carry out a quantum computation for them such that the client's inputs, outputs and computation remain private. Recently we proposed a universal unconditionally secure BQC scheme, based on the conceptual framework of the measurement-based quantum computing model, where the client only needs to be able to prepare single qubits in separable states randomly chosen from a finite set and send them to the server, who has the balance of the required quantum computational resources. Here we present a refinement of the scheme which vastly expands the class of quantum circuits which can be directly implemented as a blind computation, by introducing a new class of resource states which we term *dotted-complete graph states* and expanding the set of single qubit states the client is required to prepare. These two modifications significantly simplify the overall protocol and remove the previously present restriction that only nearest-neighbor circuits could be implemented as blind computations directly. As an added benefit, the refined protocol admits a substantially more intuitive and simplified verification mechanism, allowing the correctness of a blind computation to be verified with arbitrarily small probability of error.

Joseph Fitzsimons
National University of Singapore

Date submitted: 10 Nov 2011 Electronic form version 1.4