Abstract Submitted
for the MAR12 Meeting of
The American Physical Society

Experimental demonstration of blind quantum computing STEFANIE BARZ, VCQ, University of Vienna; IQOQI, Austrian Academy of Sciences, Austria, ELHAM KASHEFI, School of Informatics, University of Edinburgh, UK, ANNE BROADBENT, Institute for Quantum Computing, University of Waterloo; Department of Combinatorics & Optimization, University of Waterloo, Canada, JOE FITZSIMONS, Centre for Quantum Technologies, National University of Singapore, Singapore; School of Physics, University College Dublin, Ireland, ANTON ZEILINGER, PHILIP WALTHER, VCQ, University of Vienna; IQOQI, Austrian Academy of Sciences, Austria — Quantum computers are among the most promising applications of quantum-enhanced technologies. Quantum effects such as superposition and entanglement enable computational speed-ups that are unattainable using classical computers. The challenges in realising quantum computers suggest that in the near future, only a few facilities worldwide will be capable of operating such devices. In order to exploit these computers, users would seemingly have to give up their privacy. It was recently shown that this is not the case and that, via the universal blind quantum computation protocol, quantum mechanics provides a way to guarantee that the user's data remain private. Here, we demonstrate the first experimental version of this protocol using polarisation-entangled photonic qubits. We demonstrate various blind one- and two-qubit gate operations as well as blind versions of the Deutsch's and Grover's algorithms. When the technology to build quantum computers becomes available, this will become an important privacy-preserving feature of quantum information processing.

Stefanie Barz
VCQ, University of Vienna; IQOQI,
Austrian Academy of Sciences, Austria

Date submitted: 25 Nov 2011 Electronic form version 1.4