Experimental Demonstrations of Quantum Crypto
Summer & Fall 2017

Carl Miller (with Paulina Kuo)

May 30, 2017

We tentatively planning to conduct Bell type experiments on the NIST Gaithersburg campus (Chemistry Bldg., second floor). These experiments will not be as ambitious as the Boulder experiments (in particular, they will not be loophole free). The goals are to produce experimental research on quantum crypto and to help with the development of the randomness beacon.

Goal 1: Conduct experimental demonstrations of recent theoretical proofs in quantum crypto.

I've written a number of quantum cryptography papers recently which are related in one way or another to Bell inequality violations. Topics include:

1. Device-independent key distribution [3].
2. Rigidity [4] (i.e., device-independent verifications of Bell states).
3. Blind random number generation from Bell inequalities [6, 5] (i.e., generating random numbers from one detector in a Bell experiment that are unknown to the other detector.)
4. New graphical proof methods for quantum cryptography [1].
5. Steering [2] (i.e., demonstrations of nonlocality in which one the measurement devices is trusted and the other isn't).

We plan to do experimental demonstrations supporting each of these papers. ((1) and (3) are cryptographic tasks that are meant to be done by distant parties, but we'll do simulations in the lab.)

Goal 2: Create a quantum source for the randomness beacon.

We will try to create a sustained Bell violation experiment which is vulnerable to the locality loophole (since it's all going to be in a single lab) but closes other loopholes if possible. If this succeeds we'll try to plug it into the beacon.

(This will just be an intermediate step — the final goal is to have a fully loophole-free Bell experiment as the source for the beacon, and I assume that would be done by the folks in Boulder.)

References

[1] Spencer Breiner, Carl A. Miller, and Neil J. Ross. Graphical methods in device-independent quantum cryptography. arXiv:1705.09213, May 2017.

[2] Roger Colbeck, Carl A. Miller, and Yaoyun Shi. One-dimensional steering and keychain models. Forthcoming, 2017.

[3] Rahul Jain, Carl A. Miller, and Yaoyun Shi. Parallel device-independent quantum key distribution. arXiv:1703.05426, March 2017.

[4] Amir Kalev and Carl A. Miller. Rigidity of the magic pentagram game. arXiv:1705.06649, May 2017.

[5] Carl A. Miller and Yaoyun Shi. Certified randomness between mistrustful players. arXiv:1610.05140, October 2016.

[6] Carl A. Miller and Yaoyun Shi. Certifying the absence of quantum nonlocality. arXiv:1608.01011, August 2016.