A Quantum Approach to Hardware Security

PI: Yaoyun Shi, University of Michigan
Co-PIs: Carl A. Miller, NIST & University of Maryland; Kim Winick, University of Michigan

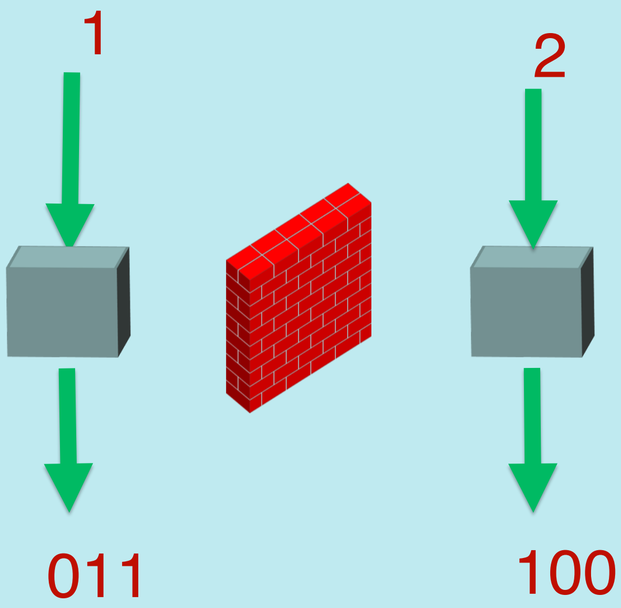


Project URL: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1526928

Objective: Solve central problems in information security through the groundbreaking approach of **device-independent quantum cryptography**.

There are at least two vulnerabilities in most current information security solutions: they are based on **unproven computational assumptions**, and they may break down if hardware components are **imperfect or maliciously designed**. Theoretical results in quantum information from the last decade have now reached a level that allows us to create revolutionary solutions to both of these problems. Our goal is to bring these solutions into practice.

Quantum cryptography exploits the unique properties of quantum physics, including quantum nonlocality, which allows us to verify cryptographic security without having to assume the accuracy of the devices. Quantum cryptography offers **trustworthy** solutions.



When two quantum devices successfully perform a Bell experiment, their outputs are guaranteed to be **random** and **correlated.** This is the basis for creating secure shared secrets.

Approach

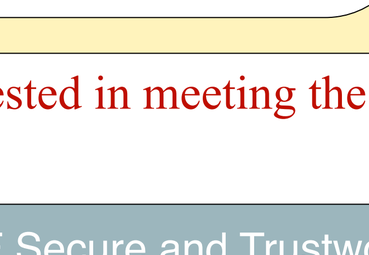
Central Problems:
Secret key **generation**
(random number generation)
Secret key **distribution**
Randomness **amplification**
(weak randomness -> perfect random key)

Goals:
-Create an experimental realization of known protocols (inc. Miller and Shi's work).
-Develop new theory to lessen the demands placed on the experiment.
-Prove new cryptographic protocols.

The Experiment

We have constructed a Bell's test apparatus consisting of a 400 nm pump UV laser, a BBO nonlinear crystal, polarization control elements and 4 single photon detectors.

The BBO crystal generates pairs of polarization entangled photons (i.e., |HH> + |VV>) at approximately 800 nm by spontaneous, parametric downconversion. We are in the process of measuring the efficiency of the single-photon detectors, which is estimated to be about 70%, and performing correlation measurements.



The inclusion of products of this photo does not imply any endorsement by NIST

Randomness Amplification from No-Signaling

PI Shi (with colleagues X. Wu and K. Chung) successfully proved that randomness amplification is possible based only on no-signaling assumptions.

Protocol [QIP 2017].

- A weak randomness source X is used as the input to many copies of a classical *randomness extractor*, each copy using a different, fixed seed.
- The output is then used for playing a non-local game.
- The final output is the XOR of all game outputs.
- The protocol accepts when a sufficient number of games were won.

Blind Randomness Expansion

Unbounded random number expansion will be possible from 3 devices, if we can prove *blind* randomness expansion (i.e., that the outputs of one device in a Bell experiment are sufficiently random to the other). PI Shi and Co-PI Miller successfully proved a one-shot version of this fact (arXiv:1610.05140, 2016).

Next steps

- Complete the Bell experiment and conduct trials of randomness generation, key distribution, and randomness amplification. Improve theory to meet experimental demands.
- Complete a proof of blind randomness expansion.
- Prove randomness generation and key distribution for **parallel** (rather than **sequential**) Bell experiments.
- Optimize!

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

UNIVERSITY OF MICHIGAN