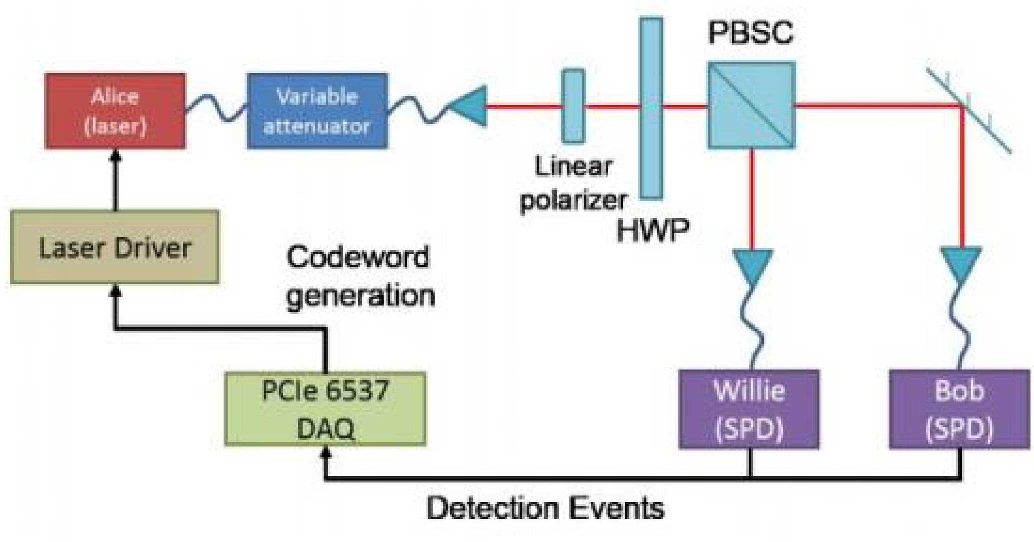
# Researchers develop covert optical communication system

May 12 2014, by Bob Yirka




Experimental setup used. Credit: arXiv:1404.7347 [cs.IT]

(Phys.org) —A team of researchers working at the University of Massachusetts has developed a way to prevent eavesdroppers from knowing when an electronic message has been communicated. In their paper, uploaded to the preprint server *arXiv*, the researchers describe a technique they've developed for hiding the presence of messages by chopping them into pieces, sending them in time blocks and hiding them in normal background noise.

Headlines of late have documented the strides made in encrypting messages using quantum mechanics—such messages are provably safe, yet, work continues because in some cases, those working covertly, wish to be able to send messages without them being noticed at all by those listening in.

Scientists know how to send messages in some circumstances that are hidden—sending a never ending stream of data across a fiber cable, for example, time sliced in prearranged patterns, prevents a listener from knowing when an actual message has been sent. But such communications wouldn't work in a truly covert operation where the need to mask all communications is critical. That's where the team working at UM came in, they devised an optical messages sending system that can send a message from one place to another, that cannot be detected at all by someone else listening in, even if the listener actually intercepts the optical signals.

The system works by subdividing time into prearranged units or bands—it's called pulse position modulation—photonic messages can be sent like Morse code and recognized by the proper receiver due to prearranged symbols assigned to the bands. But, that's only half of the secret. The other half relies on the accuracy of photon readers. Even the best detectors today are not 100 percent accurate. Sometimes they report a photon strike when none has occurred—this "noise" in the system has been found to occur at a regular rate. The researchers simply devised a system that broadcasts at the same, or lower rate. That means that if an optical message is sent, an interloper would not be able to tell if it was part of a message, or simply normal optical noise. The proper receiver, on the other hand, because of the prearrangements, would know when the message was sent, and how to read it.

The idea works as proposed—the team actually built such a system and tested it. The main drawback to such a system, though, is the need for prearranged communications. Thus, it's not clear if such a system would ever truly be useful in undercover operations.

**More information:** Covert Optical Communication, arXiv:1404.7347 [cs.IT] [arxiv.org/abs/1404.7347](arxiv.org/abs/1404.7347)

**Abstract**
Optical communication is well-suited to low probability of detection (LPD) applications. Several practical LPD systems exist that leverage the narrow beam spread at optical frequencies, and spread-spectrum modulation formats. We recently proved that theoretically one can send O(n√) bits reliably and covertly over n modes of a lossy optical channel with non-zero excess noise present either in the channel or in the adversary's receiver when the adversary Willie is assumed to be able to intercept all the light transmitted by Alice not received by the intended receiver Bob. In this paper we present the theory and implementation of optical LPD communication using a pulse position modulation (PPM) alphabet and a Reed-Solomon outer code. We prove that, when the receiver and the adversary are both equipped with photon counting receivers with non-zero dark count rates, Alice can reliably transmit O(n√logQ) bits over a lossy channel using n symbols of a Q-ary PPM constellation with essentially zero probability of detection by Willie, even if Willie can intercept all transmitted photons not received by Bob. We corroborate our theoretical result with an experiment on an optical testbed, which we believe is the first proof-of-concept demonstration of information-theoretically secure LPD communication.

via [TechnologyReview](TechnologyReview)