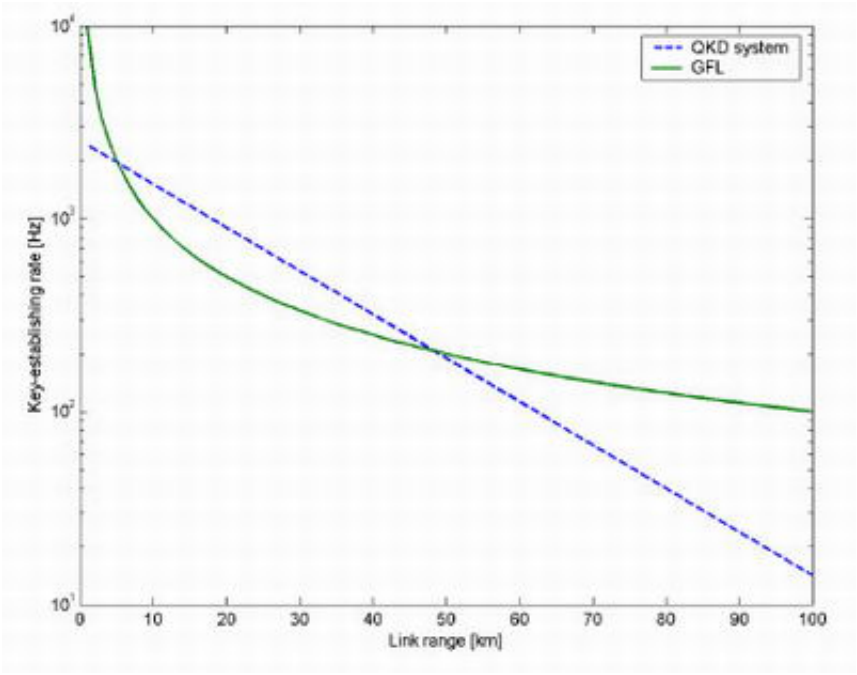
Classical cryptography system uses giant lasers to boost security

October 19 2006



This graph compares the speed it takes for establishing secret keys in a both a quantum key distribution system and the new giant fiber laser system. As the distance increases to more than 48 km, the classical laser system demonstrates its advantages, especially at longer distances. Credit: Scheuer and Yariv.

It's been more than 20 years since quantum cryptography systems have been developed, taking over communication security from classical cryptography systems--the kind that used extremely difficult mathematical equations. Now, however, scientists Jacob Scheuer and

Amnon Yariv have designed a new kind of classical key distribution system using ultra-long lasers that overcomes the practical challenges faced by quantum systems with its realistic simplicity and symmetry.

"The idea that symmetry properties can be exploited for such an objective is very appealing--symmetry is one of the deepest and most fundamental concepts in nature," Scheuer told *PhysOrg.com*. "I think there is no dispute about the importance of secure communication systems. Without a practical method enabling fast and simple secure communication, the financial system of our world--especially e-commerce and internet-based transactions--would collapse, sending us back to the middle ages."

Current quantum key distribution systems, which use the Heisenberg Uncertainty Principle, are high-tech methods that allow information to be received by a single intended recipient, who automatically alters the content upon reading it. While theoretically secure, quantum systems can fail due to challenges in practical implementation: most systems require single photons (or one entangled pair) to be emitted from a laser, and even one extra photon can put the key at risk for interception. The advantage that quantum systems do have is that, if they did work perfectly, communicators could detect an eavesdropper in a split second, making these systems extremely secure in an ideal world.

Scheuer, from Tel-Aviv University, and Yariv, from the California Institute of Technology, have designed a system that uses ultra-long fiber lasers and mirrors to achieve secure communication that is faster, better at longer ranges (above 48 km), and more difficult to intercept than quantum mechanics-based systems. Although users can't easily detect an eavesdropper here, the system increases the difficulty of eavesdropping "almost arbitrarily," making detecting eavesdroppers almost unnecessary.

"Detection of a passive eavesdropper is something unique to quantum

mechanics and to the fact that quantum particles cannot be measured without their properties being altered," said Scheuer. "However, if we can ensure that the security of the system technologically prevents Eve from gaining information of the key, we do not really care whether she tries to eavesdrop or not."

In many secure communication systems, two users need to create a secret key before sharing information. How to distribute that key--without having to use another key, ad infinitum--is the crux of a good security system. Scheuer and Yariv's concept for key distribution involves establishing a laser oscillation between the two users, who each decide how to reflect the light at their end by choosing one of three mirrors that peak at different frequencies.

Before a key is exchanged, the users reset the system by using the first mirror. Then they both randomly select a bit (either 1 or 0) and choose the corresponding mirror out of the other two, causing the lasing properties (wavelength and intensity) to shift in accordance with the mirror they chose. Because each user knows his or her own bit, they can determine the value of each other's bits; but an eavesdropper, who doesn't know either bit, could only figure out the correlation between bits, but not the bits themselves. Similar to quantum key distribution systems, the bit exchange is successful in about 50% of the cases.

"For a nice analogy, consider a very large 'justice scale' where Alice is at one side and Bob is at the other," said Scheuer. "Both Alice and Bob have a set of two weights (say one pound representing '0' and two pounds representing '1'). To exchange a bit, Alice and Bob randomly select a bit and put the corresponding weight on the scales. If they pick different bits, the scales will tilt toward the heavy weight, thus indicating who picked '1' and who picked '0.' If however, they choose the same bit, the scales will remain balanced, regardless whether they (both) picked '0' or '1.' These bits can be used for the key because Eve, who in this analogy

can only observe the tilt of the scales, cannot deduce the exchanged bit (in the previous case, Eve could deduce the bits). Of course, there are some differences between the laser concept and the scales analogy: in the laser system, the successful bit exchanges occur when Alice and Bob pick opposite bits, and not identical; also, there is the third state needed for resetting the laser, etc. But the underlying concept is the same: the system uses some symmetry properties to 'calculate' the correlation between the bits selected in each side, and it reveals only the correlation. For Alice and Bob, this is enough--but not for Eve."

To analyze the security of the ultra-long fiber laser system, Scheuer and Yariv investigated the possible methods an eavesdropper might employ. If, for example, an eavesdropper tried to determine a bit by separating the two users' waves with a beam splitter, the waves would actually appear indistinguishable, even though they come from different mirrors. Also, examining the wave spectrum would avail nothing since inline filtering can reduce the difference between the two spectra so as to make them technologically impossible to separate. In fact, the scientists found that injecting optical noise into the system from a broadband source would make an eavesdropper's measurements increasingly difficult, but still preserve the laser oscillations between users.

"The system can be significantly improved from the key-establishing and range aspects by using the same fiber to distribute many bits, using different wavelengths, simultaneously," Scheuer added. "To my knowledge, the longest fiber laser demonstrated is about 100 km long. However, 'til now there was no real incentive to develop long lasers, so I do not believe this is the limit. In principle, as long as there is enough gain (i.e., enough amplifiers), the laser could be as long as one likes."

Citation: Scheuer, Jacob and Yariv, Amnon. "Giant Fiber Lasers: A New Paradigm for Secure Key Distribution." *Physical Review Letters*. 97, 140502 (2006).

By Lisa Zyga, Copyright 2006 PhysOrg.com