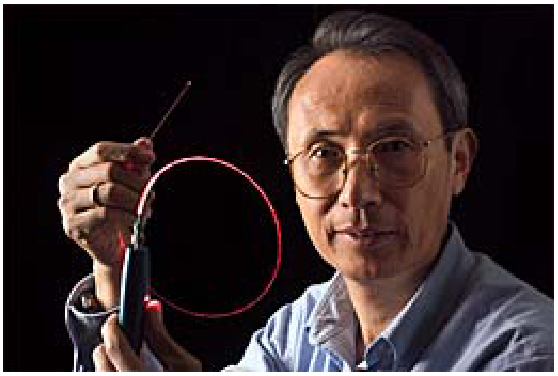
Code for 'Unbreakable' Quantum Encryption Generated at Record Speed over Fiber

April 18 2006

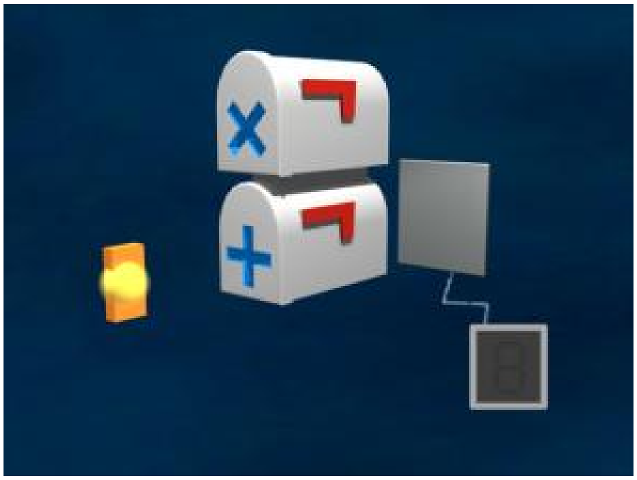


NIST physicist Xiao Tang and colleagues have developed a quantum communications system that uses single photons to produce a "raw" encryption key at the rate of 4 million bits per second. Image credit: © Robert Rathe

Raw code for "unbreakable" encryption, based on the principles of quantum physics, has been generated at record speed over optical fiber at the Commerce Department's National Institute of Standards and Technology. The work, reported today at the SPIE Defense & Security Symposium in Orlando, Fla.,* is a step toward using conventional high-speed networks such as broadband Internet and local-area networks to transmit ultra-secure video for applications such as surveillance.

The NIST quantum key distribution (QKD) system uses single photons, the smallest particles of light, in different orientations to produce a continuous binary code, or "key," for encrypting information. The rules of quantum mechanics ensure that anyone intercepting the key is detected, thus providing highly secure key exchange. The laboratory system produced this “raw” key at a rate of more than 4 million bits per second (4 million bps) over 1 kilometer (km) of optical fiber, twice the speed of NIST’s previous record, reported just last month.** The system also worked successfully, although more slowly, over 4 km of fiber.

The record speed was achieved with an error rate of only 3.6 percent, considered very low. The next step will be to process the raw key, using NIST-developed methods for correcting errors and increasing privacy, to generate "secret" key at about half the original speed, or about 2 million bps.



NIST has previously encrypted, transmitted and decrypted Web quality streaming video using secret keys generated at 1 million bps in a 1-km fiber QKD system using a slightly different quantum encoding method.*** Using the same methods for correcting errors and improving privacy with the key generated twice as fast or faster should allow real-time encryption and decryption of video signals at a resolution higher than Web quality, according to NIST physicist Xiao Tang, lead author of the paper.

View an animation that shows how single photons are sent and detected by the NIST QKD system. *(Requires Quicktime).*

“This is all part of our effort to build a prototype high-speed quantum network in our lab,” says Tang. “When it is completed, we will be able to view QKD-secured video signals sent by two cameras at different locations. Such a system becomes a QKD-secured surveillance network."

Applications for high-speed QKD might include distribution of sensitive remote video, such as satellite imagery, or commercially valuable material such as intellectual property, or confidential healthcare and financial data. In addition, high-volume secure communications are needed for military operations to service large numbers of users simultaneously and provide multimedia capabilities as well as database access.
NIST is among a number of laboratories and companies around the world developing QKD systems, which are expected to provide the next generation of data security. Conventional encryption is typically based on mathematical complexity and may be broken given sufficiently powerful computers and enough time. In contrast, QKD produces encryption codes based on the quantum states of individual photons and is considered “verifiably secure.” Under the principles of quantum physics, measuring a photon's quantum state destroys that state. QKD systems are specifically designed so that eavesdropping causes detectable changes in the system.

NIST systems are much faster, although operating over shorter distances, than previously reported QKD systems developed by other organizations. High-speed transmission is necessary for widespread practical use of quantum encryption over broadband networks. The NIST fiber QKD system was designed by physicists, computer scientists and mathematicians and is part of a testbed for demonstrating and measuring the performance of quantum communication technologies. NIST has used the testbed to demonstrate QKD in both a fiber-based system and an optical wireless system operating between two NIST buildings.

The NIST fiber QKD system has two channels operating over optical fibers that are wrapped around a spool between two personal computers in a laboratory. The photons are sent in different quantum states, or orientations of their electric field, representing 0 and 1. The system compensates for temperature changes and vibration, which could affect performance, with a NIST-designed module that automatically adjusts photon orientation on a time schedule. More extreme environmental changes are likely to occur in fibers buried or suspended outdoors as in telephone networks; the researchers plan to test a fiber QKD system in the field in the future.

After raw key is generated and processed, the secret key is used to encrypt and decrypt video signals transmitted over the Internet between two computers in the same laboratory. The high speed of the system enables use of the most secure cipher known for ensuring the privacy of a communications channel, in which one secret key bit, known only to the communicating parties, is used only once to encrypt one video bit (or pixel). Compressed video has been encrypted, transmitted and decrypted at a rate of 30 frames per second, sufficient for smooth streaming images, in Web-quality resolution, 320 by 240 pixels per frame.

The work is supported in part by the Defense Advanced Research Projects Agency.

As a non-regulatory agency of the U.S. Department of Commerce’s Technology Administration, NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Citation:
* X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. Bienfang, R.F. Boisvert, C. Clark, D. Su and C. Williams. 2006. Auto-compensated, polarization coding, fiber-based quantum key distribution system operating at sifted-key rate over 4Mbit/s. Presented April 18 at the SPIE Defense & Security Symposium, Orlando, Fla.

** X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J.C. Bienfang, D. Su, R. Boisvert, C.W. Clark and C.J. Williams. 2005. Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s. *Optics Express*. Posted online March 20.

***A. Mink, X. Tang, L. Ma, A. Nakassis, B. Hershman, J. Bienfang, D. Su, R. F. Boisvert, C. Clark, and C. Williams. 2006. High Speed Quantum Key Distribution System Supports One-Time Pad Encryption of Real-Time Video. Presented April 18 at the SPIE Defense & Security Symposium, Orlando, Fla.

Background: How the Fiber QKD Works

In the NIST fiber QKD system, a one-way quantum channel uses lasers to generate a stream of single photons, which are transmitted through an optical fiber. These photons are the carriers of the raw material for the quantum key. A two-way conventional fiber channel is used for data processing to improve the key's reliability and security. The data are processed in real time by circuit boards designed at NIST.

In the 4 million bps demonstration, the NIST system sends and receives photons in four different orientations. Each photon is sent in one of two modes, either vertical/horizontal, or plus 45 degrees/minus 45 degrees. Within each mode, one orientation represents the bit value 0, and the other represents bit value 1.

To visualize how this works, imagine that each photon is an envelope moving perpendicular to the ground (vertical=1), parallel to the ground (horizontal=0), tilted at 45 degrees to the right (plus 45 degrees =1) or tilted 45 degrees to the left (minus 45 degrees=0). Each photon fits best through one of two types of detectors, or “mailboxes.”

The sender, generally called Alice, randomly chooses both a mode and an orientation for each photon. The receiver, generally called Bob, randomly chooses between the two modes when he tries to detect a photon. This can be visualized as choosing a mailbox slot that accepts only envelopes flying in certain orientations. If he chooses the same mode that Alice used for a particular photon, then Bob always measures the correct orientation and, hence, its bit value. But if he chooses a different mailbox, then he may get the wrong bit value for that photon.

The use of optical fiber poses a special technical challenge, because Alice’s photons lose their orientation as they pass through the curved fiber. NIST researchers developed an innovative recovery method, including automatic calibration of the mailboxes, to restore the original quantum states before the photons reach Bob.

To make a shared “key” from a stream of photons, Alice tells Bob which mode she used for each photon (without revealing its bit value). Bob tells Alice which photons he actually received and measured using the correct mailbox (but again, not sharing their values). Then they both discard the other bits, the ones Bob measured with the wrong mailbox. The correct measurements constitute the initial “sifted” key (or raw key) that Alice and Bob now share. (See table below.)

If someone, generally referred to as Eve, tries to tap into the fiber and eavesdrop on the transmission, she will not be able to "read" it without leaving clues to her presence. Because of the rules of quantum physics, she cannot make perfect copies of the photons, and she would change their orientation if she tried. If she measures a photon, with the idea of sending a replacement as a cover, she may use the wrong mailbox and sometimes get the wrong bit value. She can, therefore, introduce errors in the key constructed by Alice and Bob. When Alice and Bob detect an unusual number of errors they will be alerted to Eve’s presence.

Before the sifted key is actually used, it needs to be processed further, because Alice and Bob need identical keys for reliable encryption and decryption. In a perfect world, there would be no errors or inconsistencies in their keys, unless an eavesdropper is present. But other errors, caused by environmental effects, for instance, do occur. QKD systems need to correct virtually all errors while disclosing as little information about the key as possible, because it is always assumed that Eve is listening. Conventional error-correction processes require extensive communications between Alice and Bob and are very slow. The NIST-developed method requires less interaction and is much faster.

In the NIST method, the sender and receiver’s keys are divided into segments and compared to determine whether they have even or odd numbers of 1s. These results are used to estimate the error rates in large blocks of data in the keys. These blocks are segmented based on error rates.

Then the system runs a “forward error correction” code, adapted from the telecommunication industry, on each segment with an odd number of errors. This process corrects single bit errors based on the positions of the 1s in the data. All the key bits are then shuffled, blocks are re-segmented based on the new error rates, and the correction process is repeated. This goes on until the error rate is reduced to about 1 bit per billion.

The error-corrected key is then “hashed,” or mixed up and condensed in a particular way, in the privacy amplification process. This produces a much shorter key about which Eve, statistically speaking, can know only a very small fraction. This is the secret key shared by Alice and Bob that is used for encryption and decryption.

Making a “Sifted” Key								
Alice’s bit value	1	0	0	1	0	1	1	1
Alice’s sending mode	+	+	+	X	X	+	+	+
Bob’s mailbox mode	+	X	+	+	+	+	+	X
Bob’s results	1	0	0	0	0	1	1	0
Same Mode?	Y	N	Y	N	N	Y	Y	N
Sifted Key (before error correction)	1		0			1	1	

Source: NIST

Citation: Code for 'Unbreakable' Quantum Encryption Generated at Record Speed over Fiber (2006, April 18) retrieved 24 April 2024 from https://phys.org/news/2006-04-code-unbreakable-quantum-encryption-fiber.html