cleotides, to see which ones were providing accurate information about the expected phylogenetic tree and which were causing the problems. "We wanted to see what makes a good site good and a poor site poor," Naylor says. The results were very instructive. For example, when they grouped the nucleotides into codons—nucleotide triplets that code for specific amino acids—they found that codons corresponding to the hydrophobic (water-hating) amino acids gave an "absolutely rotten" fit to the tree. On the other hand, codons for amino acids that are hydrophilic (water-loving) or carry an electric charge provided a much better fit. But the best fit of all came from amino acids that seemed to be critical for determining the proteins' three-dimensional structure.

When the analysis was rerun using only the nucleotide sites corresponding to these amino acids, the expected phylogenetic tree reemerged with considerable statistical support. Naylor concluded that rather than trying to build better trees by sequencing more and more genes—an approach common among molecular phylogeneticists—"our efforts are probably better spent investigating which kinds of sites best reflect actual historical, phylogenetic signals." Michael Nedbal, an evolutionary biologist at the Field Museum in Chicago, says Naylor's talk was "an especially important message to those in molecular phylogenetics. Just like morphologists, molecular systematists must investigate how their characters are evolving before subjecting them to phylogenetic reconstruction."

While the debate over the relative merits of molecules and morphology—and how to get the most out of each data set—is far from over, the take-home message from the Paris meeting was that each side ignores the other at its peril. Says zoologist Tim Littlewood of London's Natural History Museum: "We are all searching for a Tree of Life we can agree on."

–Michael Balter

PHYSICS

Flaw Found in a Quantum Code

With a basic principle of physics on its side, quantum cryptography seemed foolproof. Because the very act of observing a quantum system—a single photon or particle—disturbs it, any effort to crack quantum secrecy should leave a detectable trace. Or so physicists thought. In the 28 April issue of *Physical Review Letters*, researchers report with regret that another principle of quantum mechanics could undermine one quantum-cryptography scheme. The threatened scheme has never been put into practice, and the threat depends on technologies that don't exist yet outside theorists' minds. But like any blemish on something thought to be flawless, the finding has unsettled quantum cryptographers.

"I'm very disappointed with this result," says Claude Crepeau of the University of Montreal. The papers, one by Dominic Mayers of Princeton University and the other by Hoi-Kwong Lo of Hewlett-Packard and H. F. Chau of the University of Hong Kong, do not affect a basic quantum-cryptography stratagem called quantum "key exchange." In this stratagem, Alice (the sender) gives Bob (the receiver) a secret password in the form of a string of photons polarized in different directions. Any eavesdropper trying to measure the polarizations would alter them. But Mayers, Lo, and Chau have found that a quantum principle called entanglement, in which the state of one photon in a pair can reveal everything about its counterpart, can in theory be used to undermine a second quantum scheme called bit commitment.

Bit commitment gives Alice and Bob a way to exchange information even if they don't trust each other. "Suppose Alice wants to prove that she can make a prediction about the stock market, but wants to make sure that Bob can't use the information to his advantage," explains Richard Hughes, a physicist at Los Alamos National Laboratory in New Mexico. That requires a way for Alice to transmit a message to Bob while retaining control over when he can read it. "It's post–Cold War cryptography," says Charles Bennett, a cryptographer at the IBM Thomas J. Watson Research Center in Westchester County, New York. "There are no enemies anymore, but you don't trust your friends."

In a bit-commitment scheme proposed in 1984, mistrustful Alice sends a string of photons, all of them polarized diagonally, at 45 or 135 degrees, or rectilinearly at 0° or 90°. The entire string represents either a 1 (say, a series of diagonal polarizations) or a 0 (rectilinear polarizations). Bob receives each photon and randomly chooses to determine its polarization with a rectilinear or a diagonal filter. Only the correct filter will give a real measurement, but Bob can't tell when he has guessed correctly. Using the wrong filter—measuring, say, rectilinearly polarized photons with a diagonal filter—will destroy the information in the photons and yield a string of random diagonal measurements, indistinguishable from real ones.

"[The discovery] is a big disappointment for anyone interested in cryptography."
—Dominic Mayers

As a result, Bob gets no information until Alice chooses to reveal whether she sent a 1 or a 0. Bob can then verify, after the fact, that Alice really sent what she claims, by looking at the photons he measured with the correct filter. If Alice has told the truth, his readings for those photons will agree with hers. Alice can't lie, saying she sent diagonally polarized photons when they were actually rectilinear, because she has no idea what Bob saw when he used a diagonal filter. She has to guess—and because Bob randomly saw a 45° or 135° polarization, Alice will be wrong about half the time. Thus, Alice has to commit herself to a value for the bit when she sends it, but doesn't need to show her hand until later.

But there's a hole in this and all other bit-commitment schemes, the new work shows. Instead of producing each photon individually, Alice can prepare them as Einstein-Podolsky-Rosen (EPR) pairs: two photons whose polarizations are intimately linked—entangled—even as they travel in different directions. Sending a rectilinearly polarized photon to Bob, Alice stores the other without measuring it. Bob does the measurements as usual. Normally, this would mean that Alice was committed to a 0. But thanks to entanglement, she's not.

Alice can change her commitment from a 0 to a 1, or vice versa, simply by measuring each stored photon with a diagonal filter. Because her photon and Bob's make up an EPR pair, measuring one tells her all about the other; Alice thus knows what Bob's diagonal measurements were. Alice can now claim she sent a 1—a string of diagonal polarizations—and there is no way Bob can tell that she is cheating.

This scenario is still an academic exercise. For one thing, it requires the ability to store a photon without affecting its quantum state, something researchers in quantum computation are only taking the first steps toward doing. But "it's a big disappointment for anyone interested in cryptography," says Mayers, adding that it threatens a host of post–Cold War protocols designed to keep Alice, Bob, or—in some cases—both of them in the dark about parts of the information being transferred.

"It's the foundation stone which held up a useful part of quantum cryptography," agrees Bennett. "Now, it's gone, and there's no way to fix it."

–Charles Seife

Charles Seife is a writer in Riverdale, New York.