Computers

Quantum cheating

Taking advantage of quantum effects once seemed to offer a remarkably secure way of processing information. Cryptographers developed and tested schemes that appeared highly resistant to tampering and eavesdropping (SN: 2/10/96, p. 90). Now, researchers have uncovered a weakness that makes unconditional security impossible to achieve using any method that requires a specific type of quantum bit manipulation.

"This result implies a severe setback for quantum cryptography," says Dominic Mayers of Princeton University. He describes his findings in the April 28 PHYSICAL REVIEW LETTERS. Another paper on the subject, by Hoi-Kwong Lo of Hewlett-Packard Laboratories in Bristol, England, and H.F. Chau of the University of Hong Kong, also appears in that issue.

The problem involves a procedure called quantum bit commitment, which allows people to compare or combine information while keeping each individual's contribution secret. It works like this: A person writes a bit—either 0 or 1—on a piece of paper, places the slip inside a box, and locks the box. She then gives the locked box to someone else but keeps the key. She can no longer change her mind about the value of the bit. At the same time, no one else can determine her choice until she supplies the key.

The quantum version of bit commitment involves photons of polarized light. The direction of oscillation of a photon's electric field is generally given by an angle or orientation. Suppose the sender can transmit photons in four polarizations: 0° (horizontal), 45° (diagonal), 90° (vertical), and 135° (diagonal). The recipient has a choice of two measurements. One measurement distinguishes between the horizontal and vertical polarizations, and the other distinguishes between the two diagonal states.

If the recipient's detector is set up to observe only vertically polarized photons, it counts each vertically polarized photon that it sees as 1 and each horizontally polarized photon as 0. The detector's response to diagonally polarized photons is random, meaning that it is equally likely to register 1 or 0.

To make a bit commitment, the sender transmits a locked box in the form of a string of photons all polarized either vertically or diagonally. The recipient has no way of determining whether they are vertical or diagonal, so he randomly sets his detector so that it sometimes responds to vertically polarized photons and sometimes to diagonally polarized photons. Essentially, the detector records a string of 1s and 0s, which represent the correct value only when the detector happens to match the orientation of the sender's polarized photons. However, the sender can prove that she transmitted a particular orientation by obtaining the detector's setting at each point and telling him what he saw in the instances where the detector had the correct setting.

The trouble is that the sender can cheat by producing pairs of photons with the same polarization. She can then send one from each pair to the recipient and store the other for later observation. The matched photons have the curious quantum property that the observation of one affects how the other appears in a detector, an effect known as the Einstein-Podolsky-Rosen correlation. In effect, there are two linked boxes, and the sender can peek inside hers to see what the recipient has recorded at the other. Knowing all the recipient's observations, she is free to lie about whether she sent vertically or diagonally polarized photons.

"There is no way for [the recipient] to detect this attack," Lo and Chau say. Indeed, such cheating defeats all proposed schemes for quantum bit commitment, they conclude.

"Because we have shown that bit commitment is impossible," Mayers says, "we cannot hope to realize cryptographic . . . applications which are known to be powerful enough to [include] bit commitment." —*I.P.*

Earth Science

From a meeting in Baltimore of the American Geophysical Union

Florida air loaded with African dust

So much African dust blows across the Atlantic Ocean during summer that Florida and some other states on the East Coast would violate the new air quality standards proposed by the Environmental Protection Agency (EPA), reports a new study.

Researchers at the University of Miami have collected daily dust samples since 1974 from an island just off the Miami coast. Each summer, they have recorded large quantities of fine particles on days when winds carried African dust storms toward North America. The scientists can identify the source of the dust because satellite images show the progress of the storms as they cross the Atlantic. Moreover, the dust has a distinctive red-brown color, says Joseph M. Prospero.

During months when the African dust is absent, researchers measure just a few micrograms of dust per cubic meter of air. In summer, the value often surges to 50 or 100 micrograms, with the African particles accounting for most of the increase.

Current EPA regulations set standards for particles smaller than 10 micrometers in diameter, but the agency has proposed adding a different limit for particles under 2.5 micrometers. Roughly half of the African dust would meet this criterion, says Prospero. "Given the new EPA standards, it looks like Florida will be in noncompliance much of the time," he says.

The new regulations include provisions for states to exempt times when certain natural sources—such as volcanic eruptions or forest fires—boost the number of particles in the air. As yet, however, they have not included African dust as one of these exemptions. —*R.M.*

New Jersey's link to a global crisis

Not far from Atlantic City, where a roll of the dice sorts the winners from the losers, researchers report finding the best clues to date on the mass extinction that stripped fortune from the dinosaurs and bequeathed it to mammals 65 million years ago.

The new evidence comes from a borehole drilled in coastal sediments, say Richard K. Olsson and Kenneth G. Miller of Rutgers University in Piscataway, N.J., and their colleagues. Cores of sediments from the hole contain an unusually complete record of events leading up to and following this extinction, which forms the boundary between the Cretaceous (K) and Tertiary (T) periods.

Evidence collected over the last 17 years implicates a huge meteorite or comet in the extinctions at the K-T boundary. The extraterrestrial body slammed into Mexico's Yucatán Peninsula and filled Earth's atmosphere with debris, which eventually settled to form a global layer of sediment.

The New Jersey borehole contains the thickest layer of ejected material outside the Gulf of Mexico, report the Rutgers scientists. This includes a 6-centimeter-thick layer of microscopic spheres that settled onto a quiet seafloor at the end of the Cretaceous. Many scientists interpret the spheres as the remnants of molten rock sprayed into the air by the impact.

The sedimentary layers in the borehole also record the species of small ocean organisms that lived right up to the time of the extinctions, as well as the few that survived. This evidence helps tie the date of the Yucatán impact to the mass extinctions at the end of the Cretaceous, says Olsson. The link has generated debate among geologists, some of whom argue that the impact came hundreds of thousands of years earlier.

The new borehole record may not be that helpful, however, because the waning years of the Cretaceous are represented by glauconitic clay, says Gerta Keller of Princeton University. The presence of this clay indicates that the New Jersey site was in shallow water at the time of the impact and thus subject to waves that agitated the seafloor sediments. Wave activity removes sediment, thereby erasing part of the record, Keller contends. —*R.M.*