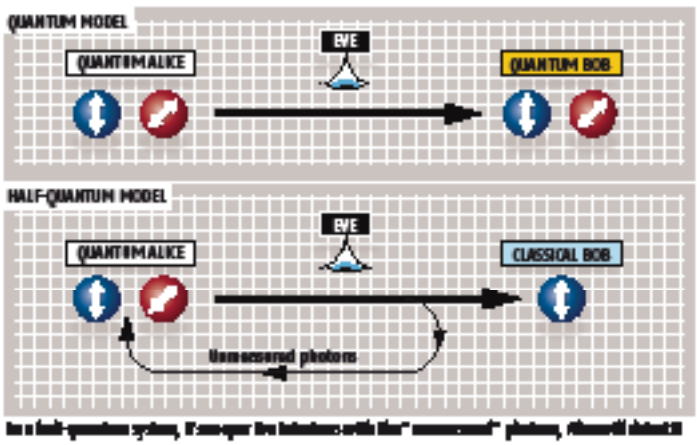
When classical Bob meets quantum Alice



IT HAS been an article of faith among cryptographers that the only way for two parties to transmit sensitive information completely securely is to use quantum cryptography to share the key they use to encrypt the information. Now it seems that the same degree of security is possible even if one party remains firmly rooted in the world of classical physics. The finding could mean simpler and cheaper secure cryptographic systems.

In the conventional model that cryptographers propose for quantum key distribution, a sender, known as Alice, generates a string of 0s and 1s and encodes them using a photon polarised in one of two ways. One way is the computational "basis", in which 0 and 1 are represented by vertical and horizontal polarisations; the other uses a diagonal basis, where 1 and 0 are represented by +45° and -45° polarisations, respectively.

When Alice's photon arrives at the receiver, called Bob, he chooses either the computational or diagonal basis to measure each one, and tells Alice which basis he has used. Whenever he uses the wrong basis, Alice tells Bob to discard that bit; the bits that are left form the secret key.

If an eavesdropper, Eve, intercepts the photons, she must guess which basis to use to read each one. As a result, the rules of quantum mechanics mean that she destroys Bob's ability to read a number of the photons that he might otherwise have read correctly. This increase in the portion of unreadable photons tells Bob that the communication channel has been compromised.

It may now be possible to get the same level of security with a system that is only half-quantum. Tal Mor at the Israel Institute of Technology in Haifa and colleagues at the University of Montreal, Canada, have shown that only Alice needs to be quantum-equipped (*Physical Review Letters*, vol 99, p 140501). "We wanted to see just how much 'quantumness' is required," says Mor.

The team set up a system with a quantum Alice, who encodes her bits according to one of two bases, and a non-quantum Bob, who can use only the computational basis to measure the photons. Bob randomly measures some of the received photons and returns the rest, untouched, to Alice. Those that Bob read that happened to be encoded in the computational basis form the key. This system is also secure: Eve doesn't know which photons will be returned to Alice unmeasured so if she interferes with any of these, Alice will know that there is an intruder. "Our hope is that classical Bob will prove as secure as the standard implementation of quantum cryptography," says Mor. **Paul Marks** ●

QUANTUM ELECTIONS

"Half-quantum" systems might one day make the benefits of quantum mechanics more widely available, but this month sees the first public test of full-scale quantum cryptography in an election.

On 21 October, the government of the canton of Geneva in Switzerland will use a quantum cryptography system costing €100,000 to safeguard its election results against data corruption or deliberate, illicit modification.

Made by ID Quantique, a Geneva-based firm that wants to commercialise quantum cryptography, the system will transmit results from the data-entry centre, where paper ballots from throughout Geneva are counted and keyed into computers, to the canton government's central data repository.

The aim, says Geneva cantonal chancellor Robert Hensler, is to "verify that the data have not been corrupted in transit between entry and storage". Next year, ID Quantique will extend the system to protect voting data entered via the web.

But David Dill, an expert in e-voting technology at Stanford University in California, does not think that this is what is needed to make elections more secure. "The transmission of the votes is not the major vulnerability. This sounds like a publicity coup for Quantique."