been identified in these organisms. They may yet turn out to have divergent Geminin homologs that operate through a different Cdt1 domain or a different protein, but it is possible that Geminin exists only in Metazoa. Geminin may have evolved to couple S-phase regulation to developmental and growth signals found only in metazoans. Given the fact that Geminin is a crucial negative regulator of the cell cycle, it will be important to establish whether it operates as a tumor-suppressor protein and whether it is mutated in cancer cells.

References

1. J. J. Blow, R. A. Laskey, *Nature* **332**, 546 (1988).
2. J. Wohlschlegel, B. Dwyer, S. K. Dhar, J. C. Walter, A. Dutta, *Science* **290**, 2309 (2000).
3. S. Tada *et al.*, *Nat. Cell Biol.*, in press.
4. S. P. Bell, B. Stillman, *Nature* **357**, 128 (1992).
5. J. H. Cocker, S. Piatti, C. Santocanale, K. Nasmyth, J. F. Diffley, *Nature* **379**, 180 (1996).
6. T. R. Coleman, P. B. Carpenter, W. G. Dunphy, *Cell* **87**, 53 (1996).
7. H. Nishitani, P. Nurse, *Cell* **83**, 397 (1995).
8. H. Nishitani, Z. Lygerou, T. Nishimoto, P. Nurse, *Nature* **404**, 625 (2000).
9. A. Whittaker, I. Royzman, T. Orr-Weaver, *Genes Dev.* **14**, 1765 (2000).
10. D. Maiorano, J. Moreau, M. Mechali, *Nature* **404**, 622 (2000).
11. T. J. McGarry, M. W. Kirschner, *Cell* **93**, 1043 (1998).

PERSPECTIVES: QUANTUM CRYPTOGRAPHY

Single Photons "on Demand"

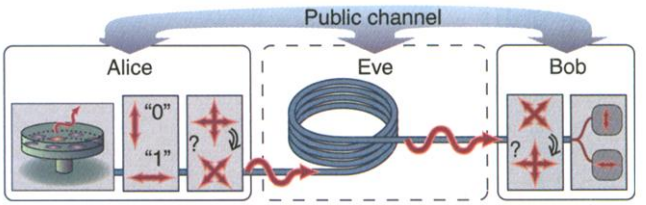
Simon Benjamin

No information without representation! This is the fundamental principle behind quantum information (*1*), a new, rapidly evolving field of physics (*2*). Information cannot exist without a physical system to represent it, be it chalk marks on a stone tablet or aligned spins in atomic nuclei. And because the laws of physics govern any such system, physics ultimately determines both the nature of information and how it can be manipulated. Quantum physics enables fundamentally new ways of information processing, such as procedures for "teleporting" states between remote locations, highly efficient algorithms for seeking solutions to equations and for factorization, and protocols for perfectly secure data transmission.

The last of these, quantum cryptography, has been fully demonstrated experimentally (*2–4*), but several obstacles have prevented its practical implementation. One of these has now been surmounted, as reported by Michler *et al.* on page 2282 of this issue (*5*) and by Lounis and Moerner in a recent issue of *Nature* (*6*). These authors have achieved, in two very different experimental setups, the generation of individual photons "on demand," thus making it essentially impossible to eavesdrop on quantum cryptographic information transfer without being noticed.

To understand why reliable generation of single photons increases the security of quantum cryptography, consider the following scenario, which is based on the protocol for quantum cryptography by Bennett *et al.* (*3*).

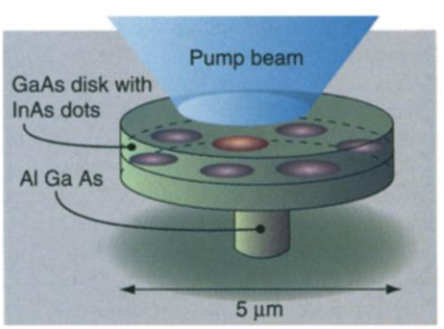
Alice wants to share a secret "key" with Bob. This key is simply a random sequence of bits; Bob will use it to encode a message, making it incomprehensible to anyone except Alice. But what if Eve tries to monitor the key's sequence without Alice and Bob's knowledge? If they exploit the physics of quantum information, Eve's eavesdropping will leave a mark. Alice distributes key bits by setting the polarization of photons horizontal or vertical (see the figure, above). She also applies a 45° "twist" to the polarization of half of the photons, chosen at random. At the receiving end, Bob also twists 50% of the photons before measuring their polarization. Then Alice and Bob openly tell each other which photons they twisted. They discard those bits that Alice has twisted and Bob has not, or vice versa. Their remaining keys will agree exactly—unless Eve has been snooping. For example, if she measured each photon and created a new one to match the result, then inevitably, 25% of Bob's final key bits will differ from Alice's. This is because Eve does not know which photons have been twisted, and so cannot untwist the right photons prior to measuring their polarization. No amount of additional cleverness or resources can avoid this effect (*7*). By publicly comparing (and then discarding) a subset of bits from their keys, Alice and Bob can thus be certain that Eve wasn't snooping, because any significant tampering will cause substantial discrepancies between those bits. Alice must not, however, send two (or more) photons at a time, because Eve could then use a simple "beam splitter attack" to measure one photon while leaving the other undisturbed (*8*).



Eavesdroppers beware! Alice, Eve, and Bob are the usual participants in quantum cryptography experiments. Eve tries to spy on the information transmitted between Alice and Bob. Controlled single-photon generation will increase the security of quantum cryptography substantially, thus moving the approach one step closer to practical implementation.

Until very recently, single photons could not be produced with very high probability. One could adjust the average number of photons in a light pulse, but a good probability of producing one photon meant that there was a similar chance of producing zero or two photons (*2*). Experimental demonstrations of quantum cryptography schemes have used pulses with an average number of photons as low as 0.1, thus minimizing the chances of multiphotons at the cost that 9 in 10 pulses contain no photons at all. Even then, however, 5% of the populated pulses will contain more than one photon. Because the pulses containing multiple photons could potentially be read undetected and Alice and Bob do not know which pulses have multiple photons, they must correspondingly shorten their key to reduce the security risk (*2*).

Michler *et al.* obtain their single photons from a quantum dot (QD) embedded in a microdisk (see the figure, left) (*5*). A related structure has been proposed by one of the authors as a possible candidate for a fully fledged quantum computer (*9*). The disk is illuminated by a laser pulse, which excites electrons in the GaAs matrix surrounding the QDs. The electrons become trapped in the QDs, together



Controlled photon release from quantum dots (QDs). A QD is a region where charge carriers become so strictly trapped that their energy levels are fully quantized, much as they are in atoms. In Michler *et al.*'s system, QDs form naturally during the growth of the layered material in which they are embedded. The material is then etched to produce a 5-μm disk containing several QDs, connected by a 0.5-μm post to the bulk sample below.

The author is at the Centre for Quantum Computation, www.qubit.org, University of Oxford, Oxford, OX1 3PU UK. E-mail: s.benjamin@qubit.org.

with the positively charged "holes" they leave behind upon excitation. The electrons and holes form composite objects called excitons, which eventually recombine, mostly by photon emission. If multiple excitons occupy a given dot, their mutual interaction ensures that all earlier recombinations occur at a different frequency than the last one. Using a monochromator to isolate the frequency of a particular dot, the structure can yield exactly one photon per laser pulse with very high probability.

The disk can also act as a high-quality optical cavity. By tuning the temperature, Michler *et al.* could adjust the frequency of emitted photons such that they were liable to being trapped by continual reflection around the circular edge. This resulted in an enhanced radiative recombination rate. Moreover, the cavity could potentially improve collection efficiency. Regrettably, the authors also found increased probability of two-photon generation.

Just a few weeks earlier, Lounis and Moerner (*6*) reported single photon generation in an entirely different system, namely single molecules (terrylene) embedded at low concentration in a micrometer-thick solid flake (*p*-terphenyl). A pump laser excites a single terrylene molecule to a higher energy excited state. This state decays very rapidly to a lower energy state, which has a half-life of nanoseconds before eventually emitting a single photon. For two photons to be emitted at this frequency, the lower state would have to decay within the 35-picosecond duration of the pump pulse. The probability of this occurrence is less than 1 in 1200. The system operates at room temperature, whereas Michler *et al.*'s QD system requires cryogenic conditions. On the other hand, in the molecular experiment, a substantial proportion of the single photon pulses are polluted by additional photons at about the same frequency from the background material. It remains unclear which approach will prove more practical.

Conventional cryptographic schemes typically rely on the difficulty of reversing certain mathematical functions (*2*), but some of these tasks would be straightforward to solve with a quantum computer (*2*). The field of quantum information therefore threatens to undermine conventional cryptography while offering a superior alternative in the form of quantum cryptography. Tremendous experimental challenges remain; for example, the range of quantum information transfer must be extended far beyond the current limit of 48 km (*4*, *10*). But the beautiful experimental achievements reported by Michler *et al.* (*5*) and by Lounis and Moerner (*6*) give good cause for optimism.

References and Notes

1. The slogan, first coined by Benjamin Schumacher, is a play on the famous colonial protest against British taxation.
2. D. Bouwmeester, A. Ekert, A. Zeilinger, Eds., *The Physics of Quantum Information* (Springer, Berlin, 2000), especially chap. 2.
3. C. H. Bennett *et al.*, *J. Cryptol.* **5**, 3 (1992).
4. R. J. Hughes *et al.*, *Advances in Cryptology—Proceedings of Crypto '96* (Springer, Berlin, 1996), pp. 329–342.
5. P. Michler *et al.*, *Science* **290**, 2282 (2000).
6. B. Lounis, W. E. Moerner, *Nature* **407**, 491 (2000).
7. D. Mayers, *Journal of the ACM*, in press, preprint available at xxx.lanl.gov/abs/quant-ph/9802025.
8. H. P. Yuen, *Quantum Semiclassic. Opt.* **8**, 939 (1996).
9. A. Imamoglu *et al.*, *Phys. Rev. Lett.* **83**, 4204 (1999).
10. W. T. Buttler *et al.*, *Phys. Rev. Lett.* **84**, 5652 (2000).
11. The author is supported by the Engineering and Physical Science Research Council.

PERSPECTIVES: PALEOCLIMATE

The Amazon Reveals Its Secrets—Partly

Julio L. Betancourt

The amount of solar irradiation received at any one time and place on Earth's surface, or insolation, is determined by long-term cyclical changes in the rotation and orbit of Earth around the sun. These insolation changes are thought to play an important role in driving global climate change, but little is known about their effects at high versus low latitudes. Did climate change in the tropics lead or lag ice volume changes at higher latitudes during global ice age cycles? And is tropical climate variability caused by changes in seasonal insolation at low latitudes, or do insolation changes at high latitudes affect the tropics indirectly through long distance effects of large-scale climate features such as El Niño–Southern Oscillation?

To answer these questions, we require reliable temperature and hydrological records for the tropics. Many tropical ocean and land records show that during ice ages, the tropics cooled by about 5°C (*1*–*4*), but tropical land records are often poorly dated and temperature and precipitation effects can seldom be distinguished. Atmospheric methane concentrations from polar ice cores are therefore frequently used as an indirect proxy for tropical paleohydrology, under the assumption that this methane comes mostly from microbial processes in tropical wetlands (*5*, *6*). Methane is also produced by sources outside the tropics, however, and the relative contribution of these different sources to past methane concentrations remains unclear.

Several recent studies have tried to reconstruct long-term changes in the South American Summer Monsoon from lake sediments (*7*, *8*), ice cores in the tropical Andes (*9*), and grassland invasions into the Atacama Desert at the southwestern limits of the tropical rainfall belt (*10*). The hope was that the Summer Monsoon's history could be used to test the validity of the tropical signals derived from the ice-core methane record, but no clear pattern emerges from these studies. Discrepancies are likely to arise from regional differences in climate over an area continental in scale.

What is clearly needed is a proxy that integrates hydrology over the entire South American tropics. Such a proxy is now provided by Maslin and Burns on page 2285 of this issue (*11*). The authors exploit the vastness of the Amazon's reach. The river drains more than 6×10^6 km^2, discharging about 20% of all fresh water that makes it into the world's oceans. It carries nearly 1 gigaton of sediment per year across the breadth of the continent and dumps it in a delta 3.3×10^5 km^2 in area with fan sediments up to 5 km in thickness. Most of the sediment originates in the Andes, but most of the water that discharges into the ocean comes from low-lying areas in the basin (*12*).

Maslin and Burns (*11*) attempt to reconstruct the past 14,000 years of the river's outflow from the oxygen isotope composition of foraminifera (single-celled marine organisms that construct calcite shells) in sediments at Ocean Drilling Program Site 942 (see the figure) (*13*). Located on the western edge of the Amazon Fan, the site is ideal for monitoring mixing of Amazon fresh water with the North Brazil Coastal Current (NBCC), the only surface water current to cross the Equator. The NBCC exports heat and salinity from the South to the North Atlantic, eventually influencing surface waters that reach the Nordic seas through the Gulf Stream. During glacial periods (and short, cold events such as the Younger Dryas), enhanced zonal winds in boreal summer could have deflected the NBCC to the southeast, shutting off cross-equatorial heat transport.

In an earlier study, Maslin *et al.* (*14*) measured the oxygen isotope composition of six foraminiferal species in the upper 4.5 m of sediment. To reconstruct Amazon outflow, Maslin and Burns (*11*) now focus on *Neogloboquadrina dutertrei*, a species that favors cooler, deeper waters and is therefore isolated from local changes in salinity. The oxygen isotope composition of *N. dutertrei*

The author is with the U.S. Geological Survey, Tucson, AZ 85745, USA. E-mail: jlbetanc@usgs.gov