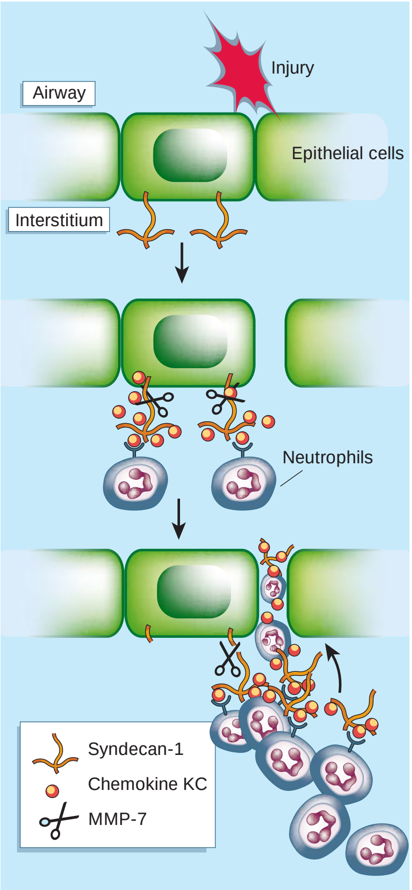

Figure 1 **Directing neutrophils to sites of injury. When damaged, epithelial cells (such as those lining the lungs) secrete the chemokine KC, which binds to syndecan-1 on an extracellular matrix scaffold[1]. Neutrophils then bind to KC. The epithelial cells also release MMP-7 (also known as matrilysin), which cleaves off the syndecan-1–KC complex. This forms a chemical gradient that directs neutrophils to the site of injury. (Figure adapted from one supplied by W. C. Parks.)**

this jigsaw puzzle. But there are still several pieces to slot into place. Why, for instance, are so many chemokines and proteinases involved in moving a limited number of cell types? How are the production and interaction of these proteins controlled? And how exactly does the sticky syndecan-1, attached to a chemokine, guide cells to their destination following cleavage? The answers might allow us to control the inflammatory process, to improve the removal of microorganisms and the repair of tissues, while limiting damage. ■

Steven D. Shapiro is at the Brigham and Women's Hospital, Harvard Medical School, 15 Francis Street, Boston, Massachusetts 02115, USA.
e-mail: sshapiro@rics.bwh.harvard.edu

1. Li, Q., Park, P. W., Wilson, C. L. & Parks, W. C. *Cell* **111,** 635–646 (2002).
2. Wilson, C. L., Heppner, K. J., Labosky, P. A., Hogan, B. L. M. & Matrisian, L. M. *Proc. Natl Acad. Sci. USA* **94,** 1402–1407 (1997).
3. Huber, A. R. & Weiss, S. J. *J. Clin. Invest.* **83,** 1122–1136 (1989).
4. McQuibban, G. A. *et al. Science* **289,** 1202–1206 (2000).
5. Senior, R. M., Griffin, G. L. & Mecham, R. P. *J. Clin. Invest.* **66,** 859–862 (1980).
6. Hunninghake, G. W. *et al. Science* **212,** 925–992 (1981).
7. Webb, L. M. C., Ehrengruber, M. U., Clark-Lewis, I., Baggiolini, M. & Rot, A. *Proc. Natl Acad. Sci. USA* **94,** 7158–7162 (1993).
8. Fitzgerald, M. L., Wang, Z., Park, P. W., Murphy, G. & Bernfield, M. *J. Cell Biol.* **148,** 811–824 (2000).

Quantum cryptography

Code-breakers confounded

Mark Hillery

Coherent-state quantum cryptography holds the promise of efficient, secure communication. An experimental demonstration shows that a secure key to the code can be exchanged, even if there is a large transmission loss.

Quantum cryptography makes use of the unusual properties of quantum mechanics to protect encoded information. In trying to listen in on a message sent through a properly designed quantum communication channel, an eavesdropper will inevitably disturb the signal and thereby reveal his or her presence. The quantum cryptographic schemes that have been explored so far have made use of either single photons or very weak light pulses. Could it be possible to use more intense light pulses containing many photons and still take advantage of quantum mechanics to protect secret information? In their paper on page 238 of this issue, Frédéric Grosshans and colleagues[1] show that it is. They have constructed a table-top system that encodes information in particular quantum states of light that contain several hundred photons each, then transmits them and decodes the information. This could lead to a faster and more efficient way of using quantum mechanics to send encrypted information.

Quantum cryptography is more accurately referred to as quantum key distribution. The codes in use today make use of both an encrypted message and a key. The key is a sequence of numbers that is known only to the legitimate sender and receiver of the message — traditionally known as Alice and Bob, respectively — and it is necessary to possess both the key and the encrypted message in order to decode the message. If the key is random and used only once, the code is unbreakable. The problem is, of course, guaranteeing that only the legitimate users know the key. This is where quantum cryptography comes in.

The first quantum key distribution system relied on encoding information in the polarization of single photons[2]. The polarization is related to the internal angular momentum of a photon, and when measured it will assume one of two possible values, which can be identified with 0 and 1. Hence the photon polarization is an example of what is known as a quantum bit, or qubit. Alice can encode the key bit in the photon polarization in many different ways. To extract the information with certainty, Bob, or an eavesdropper, must know how it was encoded. Bob makes a guess and tells Alice what his guess was. If he was right they have a key bit, if not they throw out the result. An eavesdropper, Eve, who has intercepted the photon, does not know how the key bit was encoded, and she must also guess. If she guesses incorrectly, she will introduce errors into the bits that Alice and Bob share, and by comparing a subset of these bits publicly, they can determine whether an eavesdropper was present or not.

The system constructed by Grosshans *et al.*[1] uses laser pulses containing many photons instead of single photons to carry the information about the key. The coherent pulses can be characterized by two sets of numbers: the average values of the amplitude and phase of the electric field; or the average values of the quadrature components of the electric field. If the electric field is represented by a vector in a plane, the former are equivalent to the polar coordinates of the field vector, and the latter are equivalent to its cartesian coordinates. The quadrature components obey an uncertainty relation that prevents them being accurately measured simultaneously, and, unlike qubits, they can assume a continuous range of values — they are described as continuous variables.

Several groups are investigating quantum continuous variables for effective quantum key distribution. Grosshans *et al.*[1] provide an experimental demonstration that introduces a new procedure — 'reverse reconciliation' — by which Alice and Bob handle the quantum key, encoded in continuous variables. In this scheme, Alice encodes information about the key in both quadrature components of a pulse's electric field, and Bob chooses to measure one of them. He then tells Alice which one he measured. Because Eve does not know which quadrature component Bob will measure, she has a problem; if she measures the wrong one she will introduce errors that Alice and Bob will be able to detect by comparing a subset of their key bits. The bonus is that this procedure should remain secure, in principle, even if there are signal losses during transmission: Grosshans *et al.* were able to send key bits securely at the rate of 75 kilobits per second with a transmission loss of slightly more than 50%; the rate reached 1.7 megabits for lossless transmission.

One of the things that makes quantum cryptography work is that quantum information (that is, information stored in a quantum system) cannot be exactly copied. This is known as the no-cloning theorem[3]. A consequence is that the most obvious action for an eavesdropper who has managed to intercept a message containing key bits — to make a copy of it and send the original on to the intended party — is not an option. Although it is impossible to construct perfect copies, approximate copies are allowed, but there are limits on how good the copies can be[4]. Grosshans *et al.* have explicitly demonstrated that their quantum cryptographic system is secure against an attack using the best possible coherent-state cloner.

The use of continuous variables, rather than qubits, in quantum information and computing is an expanding area of research and shows great promise[5]. Until recently, results in this area had been purely theoretical, but with the experimental demonstration of quantum key distribution and teleportation using continuous variables[6], this field of quantum information has entered the laboratory, and may soon arrive at practical applications. ■

Mark Hillery is in the Department of Physics, Hunter College, City University of New York, 695 Park Avenue, New York, New York 10021, USA.
e-mail: mhillery@hunter.cuny.edu

1. Grosshans, F. *et al. Nature* **421,** 238–241 (2003).
2. Bennett, C. & Brassard, G. in *Proc. IEEE Conf. Computers, Systems and Signal Processing* 175–179 (IEEE, New York, 1984).
3. Wooters, W. K. & Zurek, W. H. *Nature* **299,** 802–803 (1982).
4. Cerf, N. J., Ipe, A. & Rottenberg, X. *Phys. Rev. Lett.* **85,** 1754–1757 (2000).
5. Braunstein, S. L. & Pati, A. K. *Quantum Information Theory with Continuous Variables* (Kluwer, Dordrecht, in the press).
6. Furusawa, A. *et al. Science* **282,** 706–709 (1998).

Evolutionary biology

Splitting in space

Diethard Tautz

Disjunct distributions of closely related species are not necessarily the outcome of passive fragmentation of populations. Instead, they can be the consequence of speciation within a population.

Until recently, the overriding credo for explaining how new species are formed has run as follows: first, a population of organisms splits into several subpopulations; once isolated from other members of their own kind, these subpopulations become adapted to local conditions; so, over millions of years, their descendants evolve into new species. This is 'allopatric speciation', a concept in which spatial separation comes first and genetic divergence follows, and which has dominated biological thinking for many decades. The alternative, 'sympatric speciation', in which new species are created within a single population, has long been seen as a heresy — to the extent that young biologists would risk their careers if they proposed that such a mechanism could occur[1].

Over the past few years, however, modelling work[2–4] has shown that spatial separation of populations is not a prerequisite for genetic splitting. Doebeli and Dieckmann (page 259 of this issue[5]) now go even further. They propose that spatial separation is a secondary consequence of adaptive genetic divergence under sympatric conditions. In other words, splitting of a population in space can follow genetic splitting within it.

One of the strongest arguments against sympatric speciation, namely that there are no convincing mechanisms for genetic separation in sympatry, has already been addressed in the previous models[2–4]. These models solve the problem of preventing gene flow between differently adapted genotypes, a necessity if speciation is to occur, by giving the individuals an active role in choosing their mates. This is called assortative mating or mate choice, and is a well-documented phenomenon in natural populations. One model[3] suggests the parallel evolution of ecological adaptations and signals that enable individuals to recognize mating partners with genetic adaptations that are similar to their own. The other two[2,4] show that the evolution of the signals, and specific mate choice or sexual selection alone, can in themselves lead to genetic splitting.

But although there are field studies that support these models[6,7], most biologists still see sympatric splitting only as an interesting exception. This is because there is a second argument in support of allopatry: common experience shows that closely related species are usually spatially separated. If one takes this pattern as a reflection of the process, one inevitably arrives at the conclusion that, although sympatry is possible, allopatry is the norm. But this is exactly the point at which the new work will change the prevailing view.

Doebeli and Dieckmann[5] base their model on evolutionary branching[8,9], which has already shown its usefulness for understanding the sympatric splitting process[3]. Evolutionary branching describes a process, known as 'disruptive selection', under

100 YEARS AGO

We have received from the director, Captain S. S. Flower, a copy of a handy little guide (with plan) to the Zoological Gardens at Giza, near Cairo. The general introduction is written in English, French and German, and the names of the animals are given in several languages. The issue of this guide may be taken as an indication that the institution under Captain Flower's charge is in a satisfactory and progressive condition.
From *Nature* 15 January 1903.

50 YEARS AGO

***British Scientists of the Twentieth Century.* By J. G. Crowther. The book gives the impression that it is the work of two authors. There is *A*, the gifted writer with a neat and clear style, and with a wide reading in the literature of science, particularly in the biographies and publications of his characters; and there is *B*, the Marxist philosopher, ever seeking an opportunity to despise British intelligence, British institutions and British theoretical physics. Most of the writing is done by *A*, but *B* always has the last word. Some examples will show how this schizophrenic method of biography works itself out.**

J. J. Thomson. *A*: "J. J. was not only a teacher and discoverer, he was a creator in the method and organization of research .... This world-wide movement of research students to Cambridge was stimulated by the need for science teaching..." *B*: "The cost to mankind as a whole of a leisured life for Newton, Clerk Maxwell and the scores of geniuses who created the subtlety and depth of the Cambridge tradition was great .... It is impossible to overlook the adolescent, uncultivated, unintellectual aspect of his mind and school".

Rutherford. *A*: "Rutherford departed suddenly in the midst of a healthy, happy, triumphant and glorious life". *B*: "An unconsciously tragic social figure".

Jeans. *A*: "Why was Jeans so successful as a popular writer? Because he was clear, vivid, confident". *B*: "The enormous circulation of 'The Mysterious Universe' owed much to its meretricious style and shallow philosophical thought .... Somehow or other, though, Jeans extracted £256,000 out of society .... The character of his writing for the people, revealed the intellectual bankruptcy of the British educated bourgeoisie".
From *Nature* 17 January 1953.