# Practical Quantum Cryptography

**Bruno Huttner**
Université de Genève, GAP-optique. Genève, Switzerland

In so-called private-key cryptographic systems, secure transmission of confidential information through unprotected channels relies on the exchange of secret keys, known only to the sender, Alice, and the receiver, Bob. Quantum cryptography is based on the properties of quantum mechanics to obtain a provably secure key distribution. Most existing implementations rely on either the polarization or the phase of very weak pulses of light sent through optical fibers. Recent results by research groups in British Telecom, Los Alamos National Laboratory and at the University of Geneva, have shown that quantum key distribution is possible over distances of tens of kilometers, using only standard telecom cables. However, due to birefringence and the effects of the environment, the polarization at the output of a fiber fluctuates randomly. Therefore, all existing systems need active polarization control. Systems based on phase also require interferometric detection, which necessitates active stabilization of the interferometers.

To eliminate these problems, our team, led by Prof. N. Gisin in the Group of Applied Physics at the University of Geneva, is currently developing a new interferometric system implementing phase-encoded quantum key distribution (US patent pending). A schematic of the setup is given in Fig. 1. Its main features are:

1) The system is based on time-multiplexing, the interfering pulses following exactly the same spatial path, albeit with a small time delay. The interferometer is thus automatically aligned, and needs neither adjustments nor stabilization of the path lengths.

2) Use of Faraday mirrors enables all birefringence effects in the fibers to be cancelled out. Therefore, the system does not require any polarization control.

With this new system, Alice and Bob could exchange their cryptographic keys through standard telecom systems. They would be provided with a sending kit and a receiving kit, and could simply plug them in at the end of the fiber, synchronize their signals, and start the exchange. This is the reason why we refer to our system informally as a "plug and play" system. Our first experimental results show very good stability, and high fringe visibility: we measured a fringe visibility of 0.9984 over a 23 km long interferometer, based on an optical fiber used for telecommunication between Geneva and Nyon. This shows that our new scheme is indeed very promising for practical implementation of quantum cryptography. We are now working on a fully operational prototype.

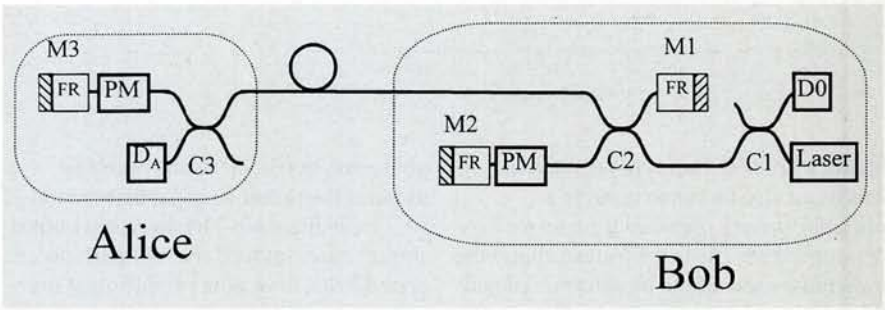


**Fig. 1.** A short laser pulse sent by Bob is split into two at coupler C2. The first part, P1, goes straight to Alice, whilst the second, P2, is delayed by the M2-M1 delay line. Alice measures the intensity of the incoming pulses in $D_A$, and attenuates them to single-photon levels. The phase modulators (PM) modulate the path length between the two pulses. On arrival back at Bob's side, part of P1 is delayed by M1-M2, and thus interferes with the incoming P2. The interference pattern at D0 gives the relative phase settings of Alice and Bob. For example, let us assume that Alice and Bob choose randomly between 0 and $\pi$ phase shifts, coding for bit value 0 and 1. If one of them chooses 0 and the other $\pi$, the interference is destructive, and no light is detected in D0. Therefore, if Bob detects a pulse in D0, he knows that Alice used the same phase shift. The Faraday rotators (FR) infront of the mirrors rotate the polarization by 45°. The effect of the combination of an FR and a mirror, known as a Faraday mirror, is thus to transform any polarization into its orthogonal. This enables all birefringence effects in the fibers to be cancelled out.

---

**Press Release**

## Digital Instruments opens East Coast Applications Lab.

With the continuing rapid growth of its customer base on the U.S. east coast, Digital Instruments has opened an East Coast Applications Lab. to provide local and more rapid response to its customers. The lab., which officially opened on 17th. March, is equipped with NanoScope® MultiMod™, BioScope™ and Dimension™ scanning probe microscopes. It is located at 223 Wilmington-Westchester Pike, Suite 114, Chad's Ford, Pennsylvania 19317. The office can be reached by (phone) 610-361-9550, (Fax) 610-361-9551, or (Email) matt@di.com, and is managed by Matt Thompson, a highly-skilled applications scientist with DI for over nine years.

According to Marketing Director, Monte Heaton, "Following on our recent opening of technical offices in Germany, Tokyo and Beijing, this new applications lab. is part of our global effort to get closer to and support our customers better. The lab. will provide applications development, user training, and product demonstrations and will allow more rapid on-site service response for our east coast customers when needed".

Digital Instruments, the world's leading manufacturer of scanning probe/atomic force microscopes, enjoyed 1995/1996 sales growth in excess of 30%, recording over $50M in sales for 1996.

For more information, contact Felicia Kashevaroff, Digital Instruments, 520 Reast Montecito St., Santa Barbara, CA 93103, Tel: (805)899-3380.