QUANTUM CRYPTOGRAPHY

Doug Wiedemann
Dept. of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario N2L-3G1

ABSTRACT. An idea of Stephen Wiesner [1] is expanded to give a method of public key distribution which is provably secure under the principles of quantum mechanics. It appears that this scheme could actually be implemented in favorable environments.

1. The Uncertainty Principle

Stephen Wiesner [1] has suggested using the uncertainty principle of quantum mechanics for 1) "A means of transmitting two messages either but not both of which may be received." and 2) "Money that it is physically impossible to counterfeit." Of these two possible applications 2) seems most clear and the idea in the present paper can be seen to be an extension of 2).

The uncertainty principle states that there exists a physical system P and features A and B which can each be measured but not both simultaneously. That is, we have the option of measuring $A(P)$ or $B(P)$, but not both. The most commonly given example is where P is a particle and A is the particle's position and B its momentum. The example we will use is where P is a photon and A its horizontal/vertical linear polarization and B its righthand/lefthand circular polarization. The advantage of this scheme is that the measured quantities are binary. That is, if we decide to measure linear polarization, the result

is *either* horizontal *or* vertical and if we decide to measure circular polarization the result is *either* righthand *or* lefthand. Once one quantity is measured it is senseless to try to measure the other. Suppose a photon has circular righthand polarization. If the linear polarization of this photon is measured the result may be horizontal or vertical. These two possibilities are equally likely. After measurement the photon is linearly polarized and the original information in the type of circular polarization has been destroyed.

2. The System

The uncertainty principle can be used to build a secure communication system for the transmission of information from a station G to a station F. Since it is apparent that this transmission will be expensive, any reasonable application would use it to securely transmit a short message, or cryptovariable, which would tell G and F how to set up a key generating device for enciphered communication over a more standard channel.

To securely send message M, assumed to be a binary stream of length l, G first selects a random binary stream, X, from $\{A,B\}^l$. Then G produces a sequence of photons such that the i^{th} photon is as follows,

1) if $M_i=0$ and $X_i=A$, horizontally polarized
2) if $M_i=1$ and $X_i=A$, vertically polarized
3) if $M_i=0$ and $X_i=B$, righthand polarized
4) if $M_i=1$ and $X_i=B$, lefthand polarized

This beam of photons is directed towards F.

To receive the message, F selects a random stream Y from $\{A,B\}^l$ and makes measurements Y_i on the i^{th} photon and converts this to a binary stream

N. Although further messages across a classical channel are now required, this is the only use of the photon channel. The classical channel will be assumed to be one where there may be eavesdropping, but where the sender of the message can be identified.

Across the classical channel F sends the message Y to G. Then G sends to F that set of values i for which $X_i=Y_i$. For these values of i $M_i=N_i$. Thus, F has received "about" half of M.

The message M should be a random binary message. Now F and G both know identical random streams, R, of length $\approx l/2$. These random bits can then be used as a "one-time-pad" or cyptovariable for a key generating device. The first thing F should do is to make some kind of verification that the photons received were the ones sent by G. This can be done by selecting a small fraction of the bits in R at random and asking G if these bits of R are correct. If a sufficient number of these are correct, F and G begin secure communication using the uncompromised portion of R. If G says that the bits don't match, G and F must begin again with new choices of M, X and Y.

3. Technical Problems

It appears that this scheme could actually be implemented using transmission of photons through space, atmosphere or fiber guide. Of course, most photon channels would be susceptible to jamming, but any attempt to eavesdrop on the photons would destroy information and cause F and G to not exchange secret information.

A major technical problem is the production of single photons of prescribed polarization. In principle this can be done, but the following modification of the G's transmission might be more practical. G uses a source that produces, say one photon every ten microseconds, on average. Each microsecond a filter over

the source is changed at random to one of four possible positions, vertical, horizontal, righthand or lefthand. This way G does not know in which time intervals a photon is sent, but given the times at which F received photons, G will know which polarization was applied. Each time F records a photon the measurement method used, A or B, should be changed with probability $1/2$, and the time should be recorded. Then F and G can compare notes and each reconstruct a random stream as before, but using the microsecond interval in place of the index i.

This method is simpler but requires synchronizing two clocks. Also, there are occasional intervals in which G sends two or more photons without knowing it. Thus, the crafty eavesdropper can occasionally recover a bit of the R stream. This is not a serious flaw because the R stream can be used in conjunction with error correcting codes and hash functions so that a few errors and a few compromised bits in R will not harm the communication method.

1. Stephen Wiesner, ``CONJUGATE CODING,'' *ACM SIGACT* **15**(1), pp. 78-88 (1983).