Quantum Cryptography:

A brief introduction to Quantum Key Distribution

Alexander Stumpf
University of New Mexico at Albuquerque 87131
Department of Physics and Astronomy

(Dated: January 23, 2000)

Abstract

The paper describes Quantum Cryptography which uses the laws of Quantum Mechanics to assure the secrecy of the communication. Furthermore, I explain implementations of Quantum Cryptography in both theory and experiment.

PACS number(s): 03.67.Dd, 03.67.-a, 89.70.+c

I. INTRODUCTION

For many years there has been a need to transmit delicate information (e.g. diplomatic, military...) over huge distances while assuring the secrecy of the data. During the last 20 years this has been achieved via public-key algorithms which use the fact that solving special mathematical problems is "difficult" and therefore the decryption of encrypted data would take longer than the time the contained information is of value. The most famous implementation is the RSA (Rivest, Shamir, Adleman) crypto-system [1] which uses the difficulty of decomposing a large number into its prime factors. It is easy to multiply, for example, the prime numbers 249187 and 1744307, but it is much harder to find the prime factors of the result, 434658628409.

With the rising probability that working quantum computers may exist in the future this problem will not be very difficult anymore as shown in [2], and an encryption such as RSA could be cracked in a couple of minutes, maybe even in seconds. This leads to the necessity of provable secure crypto-systems. But these crypto-systems (e.g. the one-time-pad [3]) all rely on a shared secret key (which has to have the same length as the plaintext message and can only be used once in order to be 100% secure) between the sender and receiver of the encrypted message. If the two parties can meet and share the key personally beforehand, they are lucky. But in the (more probable) case of having to transmit the key over a channel, the transmission has to be considered insecure - at least for "classical" means of transmission.

In 1984 Bennett and Brassard [4] developed Quantum Cryptography (or Quantum Key Distribution, QKD) which is an effort to create a secret and shared key between two parties A (normally called "Alice") and B ("Bob"). It assures that no eavesdropper ("Eve") can gain information about the key and therefore can not decrypt the final communication between Alice and Bob (which is usually transmitted via a public, i.e. theoretically insecure channel). This is described - together with the B92 protocol - in Sec. II. In Sec. III I will then show why Quantum cryptography is safe from eavesdropping, followed by Sec. IV where I will

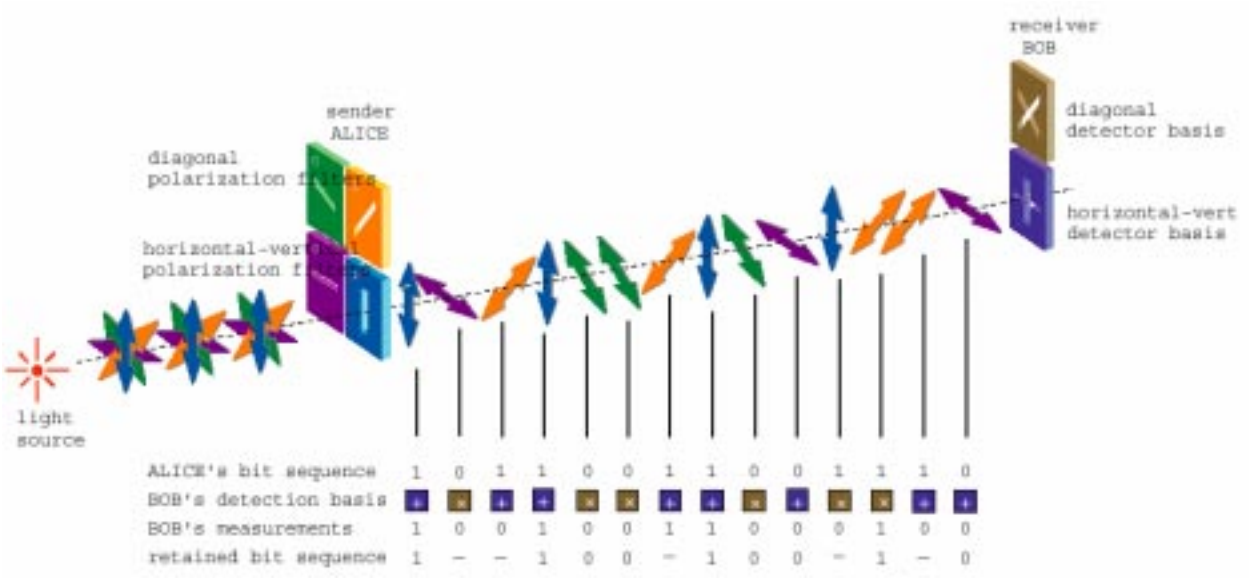

FIG. 1: The BB84 protocol by Bennet and Brassard ([4]) using horizontal, vertical, -45^o and $+45^o$ polarisations. (Figure from [10])

explain the experimental realizations performed in Geneva and Los Alamos.

II. QUANTUM KEY DISTRIBUTION

Bennett and Brassard developed in 1984 the BB84 communication protocol [4] which uses four different non-orthogonal quantum states (e.g. different polarisations of a photon) submitted via a quantum channel to transmit the bits of Alice's random key. Let us suppose she uses the vertical and the $+45^o$ polarisations for encoding the "0" and the horizontal and -45^o polarisations to encode the "1" and records each of her polarisation choices when submitting a quantum bit. Bob then randomly uses either a polarizer for diagonal polarisations or one in the horizontal/vertical basis and records his choice and the polarization he measures (Fig. 1 and Table I). The probability of using the wrong analyzer and therefore obtaining a random result is 50%.

After exchanging enough photons (i.e. more than twice the amount of bits the resulting key should have), Bob tells Alice on the public channel the sequence of analyzers he used

Alice's bits	1	0	1	1	0	0	1	1	0	0	1	1	1	0
She sends to Bob	|	—	/	|	\	\	/	|	\	—	|	/	/	—
Bob uses polarizer	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob's result	|	/	—	|	\	\	|	|	\	—	/	/	—	—
Final key data	1	-	-	1	0	0	-	1	0	0	-	1	-	0

TABLE I: Listing of states sent by Alice and measurements done by Bob according to Fig. 1

during the transmission, but not his results. Alice compares Bob's sequence with hers and tells him which bits correspond to the photons she sent. Then, only these compatible bits are used for the shared key. Table I gives an example of a possible communication between Alice and Bob. Whenever Alice sends a " | " or a "—" and Bob is using a "+"-basis detector, his measurement gives the right result and can be used for the final key, while his result is random when using the wrong, i.e. the "×"-basis for detection. For a more thorough discussion of the protocol see [4].

Another QKD-scheme has been proposed by Ekert in 1991 [5] which takes advantage of quantum correlations between Einstein-Podolsky-Rosen (EPR) pairs of particles. Alice and Bob measure randomly and independent from each other the spin of one of the EPR pairs in either, say the x- or the z-direction. After the measurement they check whether they used the same detector basis or not. If they did, their results will be opposite due to the complete anticorrelation of the EPR particles and can therefore be used for establishing a shared key similar to the BB84 protocol mentioned above (the "×"-measurement corresponding to, say a measurement of the spin in the z-direction and a measurement in the "+"-basis to one in the x-direction, respectively). In contrast to the scheme described in this paper, in Ekert's scheme there is no need to produce random numbers with a computer (which are always "pseudo-random" and therefore might decrease security) as the outcome of the measurement is not determined before the measurement is done. Furthermore, a measurement performed

	$\|\uparrow\rangle$	$\|\rightarrow\rangle$
$P_{\|\downarrow\rangle}$	0	0.5
$P_{\|\leftarrow\rangle}$	0.5	0

TABLE II: Probability to measure a "pass"

by an eavesdropper would thus increase the error rate between Alice's and Bob's key material significantly. Another advantage of using EPR pairs is the certainty of exactly one particle arriving at Alice's and Bob's detectors as opposed to an average of 0.1 photons as used in the setup described in this paper, decreasing the error rate in the key material and the sensitivity to an eavesdropper's beam-splitting attack. Please see Ekert's work and an experimental realization by Ekert *et al.* [6] for a more thorough discussion.

In 1992 Bennett published another, minimal QKD system called B92 [7] which uses only two non-orthogonal states to establish a secure connection between Alice and Bob. In this protocol, Alice again sends a random (but recorded) sequence of quantum states - say $|\uparrow\rangle$ and $|\rightarrow\rangle$ corresponding to bits "0" and "1" to Bob who measures each state he receives with either one of the projection operators $|\leftarrow\rangle\langle\leftarrow|$ ($P_{|\leftarrow\rangle}$) or $|\downarrow\rangle\langle\downarrow|$ ($P_{|\downarrow\rangle}$) also corresponding to "0" and "1" (again randomly but recorded). The probabilities of measuring a 'pass' are given in Table II.

Note that Bob will measure a 'pass' only in 50% of the bits he and Alice have in common and will never measure a pass (the probability is 0) when their bits are different. After exchanging enough bits (i.e. theoretically four times the amount of bits the final key should have) Bob tells Alice over the public channel which bits passed his measurement (but not which measurement he actually took for each bit) and these bits become the final shared key material of Alice and Bob. In the experimental realisation of this protocol the two non-orthogonal states are normally polarized photons [8] or photons with different phases [9, 10, 11].

On the following pages I will confine myself to the (two-state) B92-protocol as its experi-

mental implementation is currently much further advanced than that of the BB84-protocol. Communication distances of up to 30 km have been achieved using this two-state Quantum Cryptography protocol.

III. EAVESDROPPING

A Detecting Eve

One would probably ask why this method of key distribution is secure. Let us assume that Eve knows Alice's possible state preparations, the measurements Bob uses and that she has access to the quantum channel and can measure and replace states. I will not explain different eavesdropping strategies in this paper but restrict myself to a simple example.

Eve measures the state sent by Alice with the projection $P_{|\uparrow\rangle}$ and records a "0" if it is a pass and a "1" if it is a fail. This will identify all of Alice's 0's (state "—") correctly but also will erroneously identify 50% of her 1's as 0's. This increases the error rate between Alice's and Bob's key material from 50% to 75% which will disclose the presence of Eve. Of course there are more elaborated eavesdropping strategies, but as shown in [12, 13], the key can be used with total confidence after a procedure called "Privacy Amplification" (see III B) has been applied.

B Privacy Amplification

Because of noise generated by real detectors and erroneous detection of the wrong state there will be errors in the key data even without the presence of Eve. This necessitates a reconciliation procedure that detects and fixes these errors without revealing more information to Eve than she may already have. The so called "Privacy Amplification" described in [12] distills a smaller but error corrected key from the original private key and takes place over the public channel.

Alice and Bob agree upon a random perturbation of their bits to randomize the positions of the errors. Then they split the string into blocks of a given size which is chosen in a way that each block is unlikely to contain more than one error. Alice and Bob then compare the parity of each block and discard the last bit of each block in order to ensure that Eve does not learn anything from this process. When detecting different parity the block is divided into two smaller blocks and the parity is compared again until the error is found.

As there is still the possibility that a block contains an even number of errors (and therefore has the correct parity), this process is repeated several times with increasing block sizes until the error rate is believed to be low.

Now Alice and Bob switch to another procedure which will also be repeated several times. Instead of using blocks, this time they take a random subset of bits, compare their parity and do a bisective search for a mismatch until the error is found, again discarding the last bit of each subset in order not to disclose any additional information to Eve. Now Alice and Bob can assume their keys are identical and use it for encryption of their secret data using a provable secure encryption method (e.g. the one-time-pad [3]).

IV. EXPERIMENTAL REALIZATION

The first experimental realisation was carried out by Bennet, Bessette, Brassard, Salvail and Smolin (see [12]) over a distance of 32 cm in air in 1989. Since then, longer and longer distances have been achieved (recently, [10, 11]) using phase coding instead of polarization coding as normal telecommunication fibers change the polarization of the light while interference patterns survive somewhat better in fiber optic cables.

In Fig. 2 a schematic of the single photon interferometry setup is shown. A single photon is produced in a short wavepacket at Alice's laser source "L" and detected at Bob's detector "D". The photon exiting Alice's interferometer through the port that is linked to Bob's interferometer is a coherent superposition of a pulse that propagated through the "short" path and a time delayed pulse corresponding to the long path propagation. Each

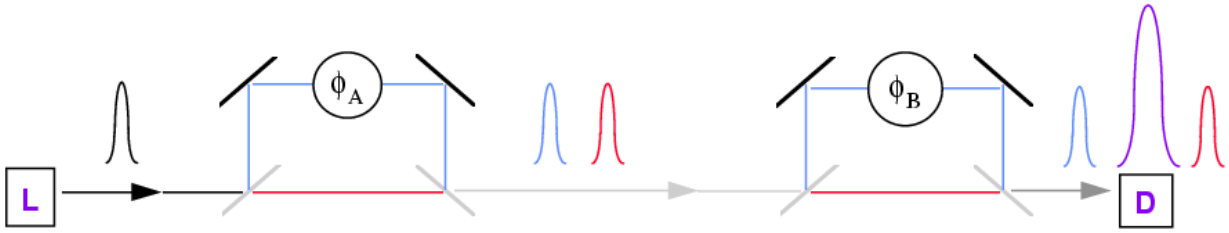

FIG. 2: Phase coding using single photon interferometry. (Figure from [11])

component is again split at Bob's interferometer, leading to three possible time windows for the photon to arrive at "D". At Bob's detector there is no interference of the short-short or long-long amplitudes, but because the path length differences in the two interferometers are identical, interference between the short-long (having relative phase Φ_A) and the long-short path (relative phase Φ_B) occurs in the central time window, being constructive for $\Phi_A - \Phi_B = 0$ and destructive for $\Phi_A - \Phi_B = \pm\pi$. So measuring constructive interference means that Alice and Bob applied the same phase shift in their interferometers (i.e. same bit in their key material).

A QKD in Los Alamos

Quantum Key Distribution has been experimentally realized in the Los Alamos Laboratories using 30 ps pulses at 1300 nm with a 10 kHz repetition rate at a distance of 1 km [11]. Alice's and Bob's interferometers were each built from a pair of 50/50 fiber couplers (see Fig. 3) with a long leg including an electro-optic non-linear crystal as phase modulator and a short leg including a variable air-gap in order to equalize the two interfering paths at Alice's and Bob's side of the interferometer. To detect the photons at Bob's side of the apparatus, a cooled InGaAs avalanche photo diode was used and the two parties were connected by a polarization-maintaining fiber because the used phase modulators were polarisation-sensitive.

The QKD-procedure itself has been carried out in the following way. First, both Alice's

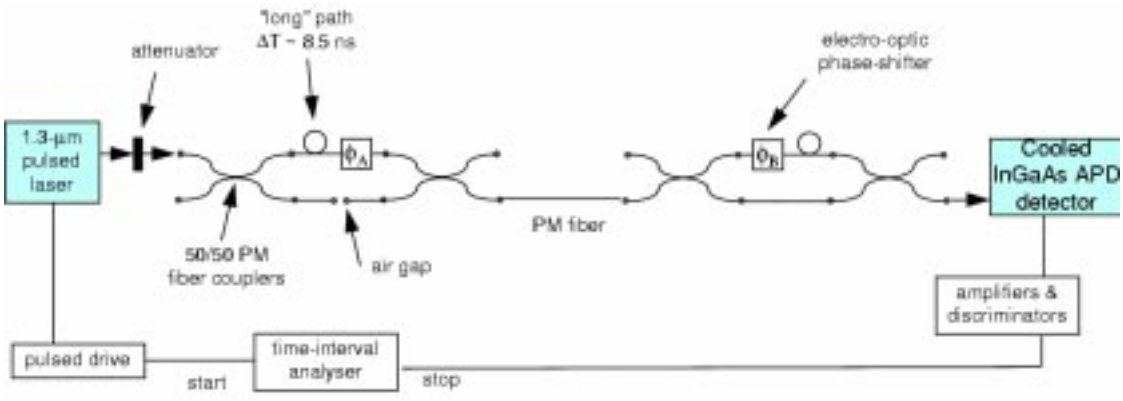

FIG. 3: Schematic representation of the optical system for the Los Alamos QKD prototype, Figure from [11]

and Bob's computers each generated a random 1024 bit-key which was loaded into the memory of a digital-analog-converter which, triggered by Alice's master clock, adjusted the phase modulators just before the laser was pulsed. At the same time the laser was pulsed, Bob's detector was triggered to open, and its output was recorded by his computer (the time coordination has been done via an ethernet connection). After all 1024 bits have been submitted, Bob sent his results to Alice using the ethernet link ($\hat{=}$ public channel) and establishing a shared key with Alice according to the B82 protocol described in II and correcting it using privacy amplification III B. This procedure was repeated until the private key was long enough to encrypt the message that was to be sent. The Quantum Cryptography group at Los Alamos is confident of being able to extend the link to a distance of 15 km transmitting any (short) message between two of the technical areas at Los Alamos.

B QKD in Geneva

The group of applied physics at the University of Geneva realized a QKD system over 23 km between Nyon and Geneva using a normal telecom fibre [10, 14]. The setup is similar to that of the Los Alamos group but in order to reduce the susceptibility to thermal drifts and polarization asymmetries in the optical fibre, a new interferometric system with Faraday

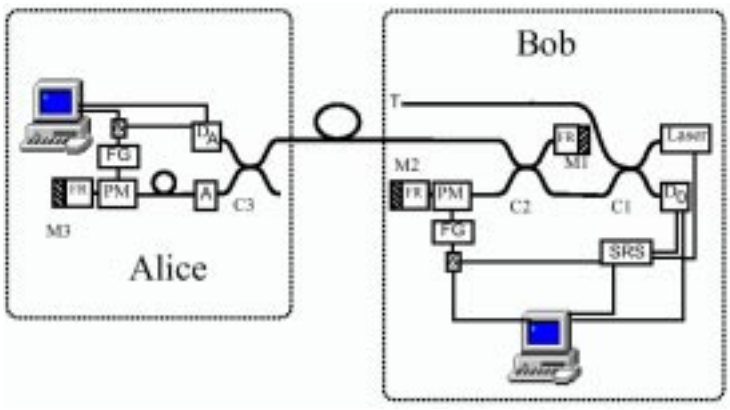

FIG. 4: Schematic diagram of the interferometric QC system (similar to Fig. 2) with Faraday mirrors, Figure from [14]

mirrors was used which removes the necessity of alignment or polarization control.

Figure 4 shows how this interferometer works [14]. It is basically an unbalanced Michelson interferometer at Bob's side, with one long arm going to Alice. The laser pulse impinging on C2 is split into two pulses P1 and P2. P2 propagates through the short arm first (being reflected at M2 first, then M1) and then travels to Alice and back. P1 is going to Alice first and passes through the short arm on its way back. As both pulses travel exactly the same path, they will interfere at C2. In order to achieve interference similar to the setup above, Alice's phase modulator only acts on P2 while Bob only modulates pulse P1, detecting constructive interference if $\Phi_A - \Phi_b = 0$ and destructive interference for $\Phi_A - \Phi_b = \pi$. The advantage of this setup is not only that the two pulses travel the same path and therefore the interferometer does not have to be aligned, but thanks to the Faraday Mirrors (FM), any birefringence (caused by arbitrary polarization transformations in each arm of the interferometer) is compensated because any light pulse reflected by a FM will come back exactly orthogonally polarized, causing both pulses to have the same polarization when finally impinging on C2. According to the authors, the setup "featured an impressive stability and a fringe visibility of 99.8%" at a bit rate of 1 Hz, letting them produce a secret key of 20 kbit length [10].

V. CONCLUSION

As shown above, practical realizations have already been achieved with impressive results and there is still much improvement possible. With further development of the equipment, distances of up to 100 km could be achieved (see [10]). On the other hand, distances far above 100 km can only be bridged using secure repeater stations. So, for long distances the practical aspect of QKD still needs to be investigated.

The author wants to thank the referees for their constructive criticism and the University of New Mexico at Albuquerque for providing the necessary equipment to get the information he needed for this paper.

REFERENCES

[1] B. Kaliski, and J. Staddon, PKCS#1: RSA Cryptography Specifications Version 2.0, RSA Laboratories, Sep. 1998, source: `ftp://ftp.rsasecurity.com/pub/pkcs/ps/pkcs-1.ps`.

[2] Artur Ekert, and Richard Josza, Quantum Computation and Shor's factoring algorithm, Rev. of Mod. Phys. **68**, 733 (1996).

[3] G.S.Vernam, and J. AIEE **45**, 109 (1926).

[4] C.H. Bennett, and G. Brassard, Quantum Cryptography: Public key distribution and coin tossing, Proc. Int. Conf. Computer Systems and Signal Processing, 175-179

(Bangalore 1984).

[5] A.K.Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[6] A.K.Ekert, and J.G.Rarity, P.R. Tapster and G.M.Palama, Phys. Rev. Lett. **69**, 1293 (1992).

[7] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[8] A.Muller, H.Zbinden, and N.Gisin, Europhys. Lett. **33**(5), 335 (1996); J.D.Franson, and B.C. Jakobs, Electron. Lett. **31**(3), 232 (1995).

[9] Ch.Marland, and P.D.Townsend, Opt. Lett. **20**(16), 1695 (1995); R.J. Hughes, G.G. Luther, G.L. Morgan, C.G. Peterson, and C. Simmons, Lecture Notes in Comput. Sci. **1109**, 329 (1996).

[10] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, Appl. Phys. **B67**, 743 (1998).

[11] Richard J. Hughes, D.M. Alde, P. dyer, G.G. Luther, G.L. Morgan, and M. Schauer, Contemporary Physics **36**, 149 (1995).

[12] C.H. Bennett, F.Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of Cryptol. **5**, 3 (1992).

[13] A.K. Ekert *et al*, Phys. Rev. **A50**, 1047 (1994); B.Huttner, N.Imoto, N.Gisin, and T.Mor, Phys. Rev. **A51**(3), 1863 (1995); C.A.Fuchs, N.Gisin, R.B.Griffiths, C.-S.Niu, and A.Peres, Phys. Rev. **A56**, 1063 (1997).

[14] H. Zbinden, J.D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, Interferometry with Faraday mirrors for quantum cryptography, preprint from Electron. Lett. 7, (03/27/97).