[102] Phoenix, S.J.D., S.M. Barnett, P.D. Townsend, and K.J. Blow, Journal of Modern Optics (1995)

[103] Rarity, J.G., P.C.M. Owens, and P.R. Tapster, **Quantum randum-number generation and key sharing,** Journal of Modern Optics, Vol. 41, No. 12, 1994, pp 2435 - 2444.

[104] Sakurai, J.J., "**Modern Quantum Mechanics**," (Revised edition), Addison-Wesley Publishing Company, Reading, Massachusetts (1994).

[105] Schumacher, Benjamin, **Quantum coding**, Physical Review A, Vol. 51, No. 4, April, 1995, pp 2738-2747.

[106] Shannon, C.E., **Communication theory of secrecy systems**, Bell Systems Technical Journal, **28** (1949), pp 656- 715.

[107] Shor, Peter W., **Algorithms for quantum computation**, preprint, pp 1 -14.

[108] Shor, Peter W., **Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Compute**, SIAM J. Computing 26 (1997) pp 1484 - . (See also quant-ph/9508027.) An extended abstract of this paper appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20–22, 1994

[109] Shor, Peter W., **Scheme for reducing decoherence in quantum computer memory**, Phys. Rev. A, Vol. 52, No. 4, October 1995, pp R2493 - 2496.

[110] Stinson, Douglas R., "**Cryptography: Theory and Practice**," CRC Press, Boca Raton, Florida (1995).

[111] Townsend, P.D., **Secure key distribution system based on quantum cryptography**, Electronic Letters, 12 May 1994, Vol. 30, No. 10, pp 809 - 811.

[112] Townsend, Paul D., and I Thompson, Journal of Modern Optics, **A quantum key distribution channel based on optical fibre**, Vol. 41, No. 12, 1994, pp 2425 - 2433.

[113] Townsend, P.D., J.G. Rarity, and P.R. Tapster, **Single photon interference in 10km long optical fibre interferometer,** Electronic Letters, **29** (1993), pp 634 - 635.

[114] Townsend, P.D., J.G. Rarity, and P.R. Tapster, **Enhanced single photon fringe visibility in a 10km-long prototype quantum cryptography channel,** Electronic Letteres, (1993) Vol. 29, pp 1291 - 1202.

[115] Townsend, P.D., S.J.D. Phoenix, K.J. Blow, and S.M. Barnett, Electronic Letters, **30**, 1994, pp 1875 - 1877.

[116] Townsend, P.D., Nature 385, p47.

[117] Wiesner, Stephen, **Conjugate coding**, SIGACT News, **15:1** (1983), p 78-88. (Manuscript circa 1970.)

[118] Williams, Colin P., and Scott H. Clearwater, "**Explorations in Quantum Computing,**" Springer-Verlag, (1998).

[119] Wootters, W.K., and W.H. Zurek, **A single quantum cannot be cloned,** Nature, Vol. 299, 28 October 1982, pp 982 - 983.

[120] Wyner, A.D., **The wire-tap channel,** The Bell Systems Technical Journal, Vol. 54, No. 8, October 1975, pp 1355 - 1387.

A Quick Glance at Quantum Cryptography

Samuel J. Lomonaco, Jr.*
Dept. of Comp. Sci. & Elect. Engr.
University of Maryland Baltimore County
1000 Hilltop Circle
Baltimore, MD 21250
E-Mail: Lomonaco@UMBC.EDU
WebPage: http://www.csee.umbc.edu/~lomonaco

November 8, 1998

Abstract

The recent application of the principles of quantum mechanics to cryptography has led to a remarkable new dimension in secret communication. As a result of these new developments, it is now possible to construct cryptographic communication systems which detect unauthorized eavesdropping should it occur, and which give a guarantee of no eavesdropping should it not occur.

Contents

*Partially supported by ARL Contract #DAAL01-95-P-1884, ARO Grant #P-38804-PH-QC, and the L-O-O-P Fund.

1 Cryptographic systems before quantum cryptography

A brief description of a classical cryptographic system (CCS) [106] is illustrated in Fig. 1.

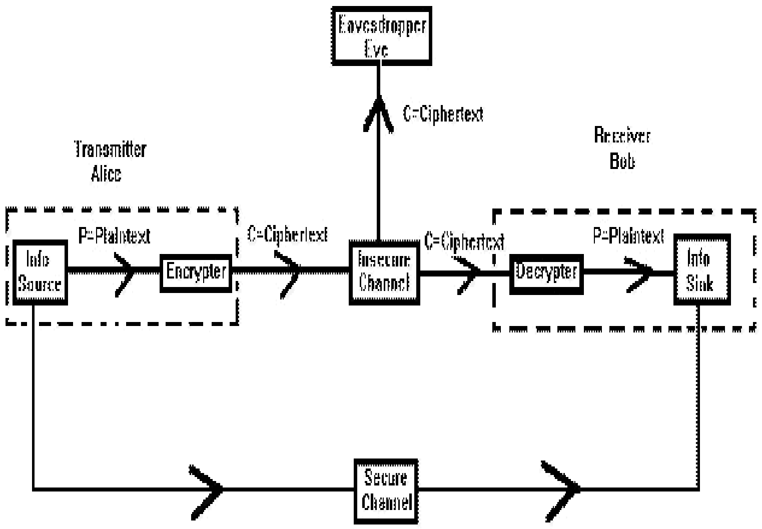


Figure 1. A classical cryptographic communication system.

A message, called **plaintext** P, is encrypted via a secret **key** K into **ciphertext** C, sent over a non-secure communication channel, and finally decrypted via a secret **key** K' back into readable plaintext P. Following the conventions of the cryptographic literature, we will refer to the transmitter as **Alice**, to the receiver as **Bob**, and to an adversarial eavesdropper as **Eve**.

There are classical cryptographic systems which are **perfectly secure** (see [106]), such as the **Vernam cipher**, better know as the **one time pad**, which uses a perfectly random key K equal in length to the length of the message. The chief practical difficulty with such perfectly secure systems is that Alice must first communicate a random key in secret via some totally secure channel. In most cases, the length of the key makes this secure communication impractical and too costly. Because of the large cost of transmitting such long keys over a secure channel, Alice is frequently tempted to use the same key twice. If she makes this fatal mistake, then her ciphertext immediately changes from being perfectly secure to ciphertext that is easily read by Eve.

Thus, for almost all practical cryptographic systems, the key K is substantially shorter than the length of the plaintext. As a result, the ciphertext is no longer perfectly secure. However, if the encryption method and key K are wisely chosen, then Alice's communication to Bob will be **practically secure**. By

[76] Hughes, Richard J., G.G. Luther, G.L. Morgan, and C. Simmons, **Quantim cryptography over 14 km of installed optical fiber**, preprint to be published in Proceedings of the "Seventh Rochester Conference on Coherence and Quantum Optics," Rochester, NY, June 1995.

[77] Huttner, B. and N. Imoto, N.Gisin, and T. Mor, **Quantum cryptography with coherent states**, Physical Review A, Vol. 51, N0. 3 (1995), 1863 - 1869.

[78] Huttner, Bruno, and Artur K. Ekert, **Information gain in quantum eavesdropping**, Journal of Modern Optics, 1994, Vol. 41, No. 12, 2455 - 2466.

[79] Ivanovic, I.D., **How to differentiate between non-orthogonal states,** Physics Letters A, Vol. 123, No. 6, 17 August 1987, pp 257 - 259.

[80] Jacobs, B.C. and J.D. Franson, **Quantum cryptography in free space**, Optics Letters, Vol. 21, November 15, 1996, p1854 - 1856.

[81] Jauch, J.M., and C. Piron, **Generalized localizability,** Phys. Acta **40** (1967), pp 559 - 570.

[82] Leung-Yan-Cheong, Sik K., and Thomas M. Cover, **Some equivalences between Shannon entropy and Komolgorov complexity,** IEEE Transactions on Information Theory, Vol. IT-24, No. 3, May 1978, pp 331 - 338.

[83] Lo, Hoi-Kwong, and H.F. Chau, **Is Quantum Bit Commitment Really Possible?**, Phys. Rev. Lett. 78, (1997), p3410-3413.

[84] Lo, Hoi-Kwong, **Insecurity of quantum secure computations**, Phys. Rev. A, 56, (1997), 1154-1162.

[85] Lo, H.-K, and H.F. Chau, **Quantum computers render quantum key distribution unconditionally secure over arbitrarily long distance**, quant-ph/9803006.

[86] Mayers, Dominic, **Unconditionally Secure Quantum Bit Commitment is Impossible**, Phys. Rev. Lett. 78, (1997), p3414-3417.

[87] Mayers, Dominic, Crypto'96, p343.

[88] Mayers, Dominic, and Andrew Yao, **Quantum cryptography with imperfect apparatus**, quant-ph/9809039.

[89] Mayers, Dominic, **Unconditional security in quantum cryptography**, quant-ph/9802025.

[90] Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone, **"Handbook of Applied Cryptography,"** CRC Press, New York (1997).

[91] Meyers, J.M., and H.E. Brandt, **Converting an operator valued measure to a design for a measuring instrument on the laboratory bench**, Measurement Science & Technology, Vol. 8 (1997), 1222 - .

[92] Mermin, N. David, **Limits to quantum mechanics as a source of magic tricks: Retrodiction and the Bell-Kochen-Specker theorem,** Physical Review Letters, Vol. 74, No. 6, 6 February 1995, pp 831 - 834.

[93] Muller, A., H. Zbinden, and N. Gisin, Europhysics Letters, 33, p. 335-.

[94] Muller,A., T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, **"Plug and play" systems for quantum cryptography**, Applied Phys. Lett. 70, (1997), 793-795

[95] Omnes, Roland, **"An Interpretation of Quantum Mechanics,"** Princeton University Press, Princeton, New Jersey, (1994).

[96] Pellizzare, T., S.A. Gardiner, J.I. Cirac, and P. Zoller, **Decoherence, continuous observation, and quantum computing: Cavity QED model,** Phys. Rev. Letters, Vol. 75, No. 21, 20 November 1995, pp 3788 - 3791.

[97] Penrose, Roger, "**The Large, the Small and the Human Mind**," Cambridge University Press, (1997).

[98] Peres, Asher, **How to differentiate between non-orthogonal states,** Physics Letters A, Vol. 128, No. 1,2. 21 March 1988, pp 19 - 19.

[99] Peres, Asher, **"Quantum Theory: Concepts and Methods,"** Kluwer Academic Publishers, Boston, (1993).

[100] Phoenix, Simon J. D., **Quantum cryptography without conjugate coding,** Physical Review Letters, Vol. 48, No. 1, July 1993, pp 96 - 102.

[101] Phoenix, Simon J., and Paul D. Townsend, **Quantum cryptography: how to beat the code breakers using quantum mechanics**, Comtemporay Physics, vol. 36, No. 3 (1995), pp 165 - 195.

[49] Diffie, W., **The first ten years in public-key cryptography**, in "Contemporary Cryptology: The Science of Information Integrity," pp 135 - 175, IEEE Press (1992).

[50] Diffie, W., and M.E. Hellman, **New directions in cryptography**, IEEE Tranactions on Information Theory, **22** (1976), pp 644 - 654.

[51] Dirac, P.A.M., "**The Principles of Quantum Mechanics**," (Fourth edition). Oxford University Press (1958).

[52] DiVincenzo, David P., **Quantum computation,** Science, Vol. 270, 13 October 1995, pp 255 - 261.

[53] Domokos, P., J.M. Raimond, M. Brune, and S. Haroche, **Simple cavirt-QED two-bit universal quantum logic gate: The principle and expected performances**, Phys. Rev. A, Vol. 52, No. 5, November 1995, pp 3554 - 3559.

[54] Dove, Chris, **Quantum computers and possible wavefunction collapse**, Phys. Letters A, 207 (1995), pp 315 - 319.

[55] Ekert, Artur K., Bruno Huttner, G. Massimo Palma, and Asher Peres, **Eavesdropping on quantum-cryptographical systems**, Phys. Rev. A, Vol. 50, No 2, August 1994, pp 1047-1056.

[56] Ekert, Artur K., and G. Massimo Palma, **Quantum cryptography with interferometric quantum entanglement**, Journal of Modern Optics, 1994, vol. 41, no. 12, 2413 - 2423.

[57] Ekert, Artur, and Richard Jozsa, **Notes on Shor's efficient algorithm for factoring on a quantum computer**, Workshop on Quantum Computing and Communication, Gaitherburh, MD, August 18-19, 1994, (preprint, 21 pages).

[58] Ekert, Artur, **Quantum keys for keeping secrets**, New Scientist, 16 January 1993, pp 24 -28.

[59] Ekert, Artur K., and John G. Rarity and Paul R. Tapster, and G Massimo Palma, **Practical quantum cryptography based on two-photon interferometry**, Physical Review Letteres, Vol. 69, No. 9, 31 August 1992, pp 1293 - 1295.

[60] Ekert, Artur K., **Quantum cryptography based on Bell's theorem,** Physical Review Letters, Vol. 67, No. 6, 5 August 1991, pp 661 - 663.

[61] Ekert, Artur, **Beating the code breakers**, Nature, vol. 358, 2 July 1992, pp. 14 - 15.

[62] van Enk, S.J., J.I. Cirac, and P.Zoller, **Purifying two-bit quantum gates and joint measurements in cavity QED**, quant-ph/9708032.

[63] van Enk, D.J., J.I. Cirac, and P. Zoller, **Ideal quantum communication over noisy channels: A quantum optical implememtation**, quant-ph/9702036.

[64] Einstein, A., B. Podolsky, N. Rosen, **Can quantum, mechanical description of physical reality be considered complete?**, Phys. Rev. **47**, 777 (1935); D. Bohm "**Quantum Theory**", Prentice-Hall, Englewood Cliffs, NJ (1951).

[65] Feynman, Richard P., Robert B. Leighton, and Matthew Sands, "**The Feyman Lectures on Physics: Vol. III. Quantum Mechanics**," Addison-Weslley Publishing Company, Reading, Massachusetts (1965).

[66] Franson, J.D., and H. Ilves, **Quantum cryptography using optical fibers,** Applied Optics, Vol. 33, No. 4, 10 May 1994, pp 2949 - 2954.

[67] Franson, J.D., and H. Ilves, **Quantum cryptography using polarization feedback,** Journal of Modern Optics, Vol. 41, No. 12, 1994, pp 2391 - 2396.

[68] Franson, J.D., and B.C. Jacobs, **Operational system for quantum cryptography**, Electronics Letters, Vol. 31, No. 3, February 2, 1995, pp. 232-233.

[69] Franson, J.D., **Quantum cryptography**, Optics and Photonics News, March, 1995, pp31-33.

[70] Glanz, James, **A quantum leap for computers?,** Science, Vol. 269, 7 July 1995, pp 28 - 29.

[71] Grover, Lov K., Proc. of 28th Annual ACM Symposium on the Theory of Computing, p212.

[72] Grover, Lov K., **How fast can a quantum computer search?**, quant-ph/9809029.

[73] Grover, Lov K., **Quantum computers can search arbitrarily large databases by a single query**, quant-ph/9706005.

[74] Herrmann, F., and G. Bruno Schmid, **An anology between information and energy,** Eur. J. Phys. **7** (1986), 174 - 176.

[75] Hughes, Richard J., D.M. Alde, P. Dyer, G.G. Luther, G.L. Morgan, and M. Schauer, **Quantum cryptography**, Contemporary Physics, Vol. 36, No. 3 (1995), pp 149 - 163.

"practically secure," we mean that, although adversary Eve is theoretically able to decrypt Alice and Bob's communication without any knowledge of their key, she can not do so because the required computational time and resources are simply beyond her capability and means. The **Data Encryption Standard (DES)** is believed to be an example of such a practically secure encryption system. (See for example [110].)

In any case, one Achilles heal of classical cryptographic communication systems is that secret communication can only take place after a key is communicated in secret over a totally secure communication channel. This is frequently referred to as the "CATCH 22" of cryptography, i.e.,

Catch 22: Before Alice and Bob can communicate in secret, they must first communicate in secret.

There is even more to this catch 22, namely:

Catch 22a: Even if Alice and Bob somehow succeed in communicating their key over a secure communication channel, there is simply no classical cryptographic mechanism guaranteeing with total certainty that their key was transmitted securely, i.e., that their "secure" communication channel is free of Eve's unauthorized intrusion.

As we shall see, quantum encryption does provide a means of circumventing this impasse of intrusion detection.

A proposed solution to the catch 22 of classical cryptographic communication systems is the modern **public key cryptographic system** (**PKCS**) as illustrated in Fig. 2. (See [49] [50].)

For public key cryptographic systems, it is no longer necessary for Alice and Bob to exchange key over a secure channel. Instead, Alice and Bob both create their own individual encryption/decryption key pairs (E_A, D_A) and (E_B, D_B), respectively. Then they both keep their decryption keys D_A and D_B secret from everyone, including each other, and "publish" or publicly broadcast their encryption keys E_A and E_B for the entire world to see. The security of such a public key cryptographic system depends on the selection of an encryption/decryption algorithm which is a **trapdoor function**. As a result, recovering the decryption key from the encryption key is computationally infeasible. The RSA public key cryptographic system is believed to be an example of such a cryptographic system. (See for example [110].)

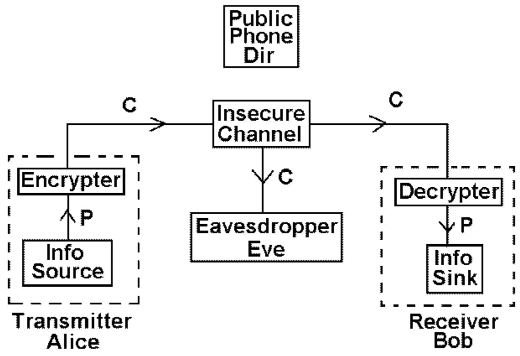


Figure 2. A public key cryptographic communication system.

One major drawback to public key cryptographic systems is that no one has yet been able to prove that practical trapdoor functions exist. As a result, no one is really sure how secure such public key cryptographic systems are. Moreover, if researchers succeed in building a feasible quantum computer, Shor's quantum factoring algorithm [108] could break RSA easily, i.e., in polynomial time.

Yet another drawback to public key cryptographic systems is that, in terms of some everyday implementations, such systems frequently do not circumvent the catch 22 of classical cryptography after all. The keys for many practical public key cryptographic systems are frequently managed by a **key bank** that is independent of Alice and Bob. Thus, secret communications over a secure channel from the key bank to Alice and Bob are required before Alice and Bob can secretly communicate.

Finally, it should be noted that the most important contribution of quantum cryptography is a mechanism for detecting eavesdropping. This is a totally new contribution to the field of cryptography. Neither classical cryptographic systems nor public key cryptographic systems have such a capability. In the next section, we will see how quantum mechanics provides a means for detecting intrusion.

2 Preamble to quantum cryptography

The recent results in quantum cryptography are based on the **Heisenberg uncertainty principle** of quantum mechanics[1]. Using standard Dirac notation[2], this principle can be succinctly stated as follows:

Heisenberg Uncertainty Principle: For any two quantum mechanical **observables** A and B

$$\left\langle (\Delta A)^2 \right\rangle \left\langle (\Delta B)^2 \right\rangle \geq \frac{1}{4} \left\| \langle [A, B] \rangle \right\|^2 ,$$

where

$$\Delta A = A - \langle A \rangle \qquad \text{and} \qquad \Delta B = B - \langle B \rangle ,$$

and where

$$[A, B] = AB - BA.$$

Thus, $\left\langle (\Delta A)^2 \right\rangle$ and $\left\langle (\Delta B)^2 \right\rangle$ are variances which measure the uncertainty of observables A and B. For **incompatible** observables, i.e., for observables A and B such that $[A, B] \neq 0$, reducing the uncertainty $\left\langle (\Delta A)^2 \right\rangle$ of A forces the uncertainty $\left\langle (\Delta B)^2 \right\rangle$ of B to increase, and vice versa. Thus the observables A and B can not be simultaneously measured to arbitrary precision. Measuring one of the observables interferes with the measurement of the other.

Young's double slit experiment is an example suggesting how Heisenberg's uncertainty principle could be used for detecting eavesdropping in a cryptographic communications. This experiment is illustrated in Fig. 3.

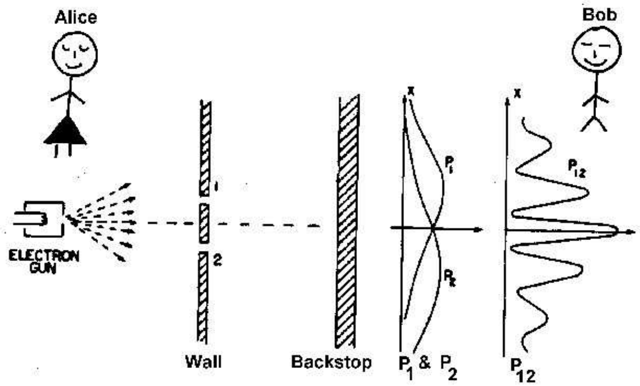


Figure 3. Young's double slit experiment when electron trajectories are not observed. The first of two incompatible observables is measured.

An electron gun randomly emits electrons over a fairly large angular spread. In front of the gun is a metal wall with two small slits. Beyond the wall is a backstop that absorbs the electrons that pass through the two slits. The probability density pattern of the absorbed electrons is described by the curves P_1, P_2, and P_{21} which, for the convenience of the reader, have been drawn behind the backstop. The curve P_1 denotes the probability density pattern if only slit 1 is open. The curve P_2 denotes the probability density pattern if only slit 2 is open. Finally, the curve P_{12} denotes the probability density pattern if both slits 1 and 2 are open. Thus, P_{12} shows a quantum mechanical interference pattern demonstrating the wave nature of electrons.

[1] For those not familiar with quantum mechanics, please refer to appendix C for a quick overview.
[2] As outlined in Appendix C

[24] Brandt, Howard E., John M. Meyers, And Samuel J. Lomonaco,Jr., **Aspects of entangled translucent eavesdropping in quantum cryptography**, Phys. Rev. A, Vol. 56, No. 6, December 1997, pp. 4456 - 4465.

[25] Brandt, Howard E., **Positive operator valued measure in quantum information processing,** preprint.

[26] Brandt, Howard E., **Eavesdropping optimization for quantum cryptography using positive operator valued measure**, U.S. Army Research Lab preprint, ARL-PP-98-5 (September, 1998).

[27] Brassard, Gilles, **Cryptology column: How convincing is your protocol?**, SIGACT News, Vol. 22, No. 1, Winter (1991) (whole Number 78), pp 5 - 12.

[28] Brassard, Gilles, **Cryptology column – Quantum computing: The end of classical cryptography?,** , SIGACT News, Vol. 93, October, 1994, pp 15 - 21.

[29] Brassard, Gilles, **Cryptology column – Quantum cryptography: A bibliography,** SIGACT News, October 1993. pp 16 - 20.

[30] Brassard, Gilles, Claude Crépeau, Richard Jozsa, and Denis Langlois, **A quantum bit commitment scheme provably unbreakable by both parties,** 34-th Annual Symposium om Foundations of Computer Science (1993), pp 362 - 371.

[31] Breguet, J., A. Muller, and N. Gisin, **Quantum cryptography with polarized photons in optical fibers: Experiment and practical limits,** Journal of Modern Optics, Vol. 41, No. 12,, 1994, pp 2405 - 2412.

[32] Briegel, H.-J., W. Dür, S.J. van Enk, J.I. Cirac, and P. Zoller, **Quantum communication and the creation of maximally entangled pairs of atoms over a noisy channel**, quant-ph/9712027.

[33] Briegel, H.-J., W. Dür, J.I. Cirac, and P. Zoller, **Quantum repeaters for communication**, quant-ph/9803056.

[34] Brillouin, L., **Physical entropy and information II,** Journal of Applied Physics, Vol. 22, No. 3, March 1951, pp 338 - 343.

[35] Brillouin, L., **Maxwell's demon cannot operate: Information and entropy I.,** Journal of Applied Physics, Vol. 22, No. 3, March 1951, pp 334 - 337.

[36] Busch, Paul, Pekka J. Lahti, and Peter Mittelstaedt, "**The Quantum Theory of Measurement**," Springer-Verlag, New York (1991).

[37] Cartan, Henri, and Samuel Eilenberg, "**Homological Algebra**," Princeton University Press, Princeton, New Jersey, (1956).

[38] Cerny, Vladimir, **Quantum computers and intractible (NP-complete) computing**, Physical Review A, Vol. 46, No. 1, July 1993, pp 116 -119.

[39] Chuang, Issac L. and Yoshihisa Yamamoto, **Simple quantum computer**, Phys. Rev. A, Vol. 52, No. 5, November 1995, pp 3489 - 3496.

[40] Collins, Graham P., **Quantum cryptography defies eavesdropping**, Physics Today, November 1992, pp 21 - 23.

[41] Coppersmith, Don, **An approximate Fourier transform useful in quantum factoring**, Workshop on Quantum Computing and Communication, Gaitherburh, MD, August 18-19, 1994, (preprint, 9 pages).

[42] Crépeau, Claude, **Quantum oblivious transfer**, Journal of Modern Optics, 1994, vol. 41, No. 12, 2445-2445.

[43] Csiszár, Imre, and János Körner, **Broadcast channels with confidential messages,** IEEE Tranactions on Information Theory, Vol. IT-24, No. 3, May 1978, pp 339 - 348.

[44] Davies, E. B., **Information and quantum measurement,** IEEE Tranactions on Information Theory, Vol. IT-24, No. 5, September 1978, pp 596 - 599.

[45] Davies, E.B., **An operational approach to quantum probability,** Commun. Math. Phys. 17, 239-260(1970).

[46] D'Espagnat, B., Scientific American, November 1979, pp 128 - 140.

[47] Deutsch, David, **Quantum communication thwarts eavesdroppers**, New Scientist, 9 December 1989, pp 25 - 26.

[48] Dieks, D., **Communication by EPR devices,** Physics Letters, Vol. 92A, No. 6, 22 November 1982, pp 271 - 272.

15 References

References

[1] Barenco, Adriano, Charles Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter, **Elementary gates for quantum computation**, Phys. Rev. A, Vol. 52, No. 5, November, 1995, pp 3457 - 3467.

[2] Barnett, Stephen M., Rodney Loudon, David T. Pegg, and Simon J.D. Phoenix, **Communication using quantum states,** Journal of Modern Optics, Vol. 41, No. 12, 1994, pp 2351 - 2373.

[3] Barnett, Stephen M., and Simon J.D. Phoenix, **Information-theoretic limits to quantum cryptography**, Physical Review A, vol. 48, no. 1, July 1993, 1050-2947.

[4] Bell, J.S., Physics, 1, (1964), pp 195 - 200.

[5] Benioff, Paul, **Quantum mechanical models of Turing machines that dissipate no energy,** Physical Review Letters, Vol. 48, No. 23, 7 June 1982, pp 1581 - 1585.

[6] Bennett, Charles H., François Bessette, Gilles Brassard, Louis Salvail, and John Smolin, **Experimental quantum cryptography**, J. Cryptology (1992) 5: 3 - 28.

[7] Bennett, Charles H., **Quantum cryptography using any two nonorthogonal states,** Physical Review Letters, Vol. 68, No. 21, 25 May 1992, pp 3121 - 3124.

[8] Bennett, Charles H., **Quantum cryptography: Uncertainty in the service of privacy**, Science, Vol. 257, 7 August 1992, pp 752 - 752.

[9] Bennett, Charles H., and Stephen J. Weisner, **Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states,** Physical Review Letters, Vol. 69, No. 20, 16 November 1992, pp 2881 - 2884.

[10] Bennett, Charles H., and Gilles Brassard, **Quantum cryptography: Public key distribution and coin tossing**, International Conference on Computers, Systems & Signal Processing, Bagalore, India, December 10-12, 1984, pp 175 - 179.

[11] Bennett, Charles H., Gilles Brassard, Seth Breidbart, and Stephen Wiesner, **Quantum Cryptography, or unforgeable subway tokens**, Crypto 1982, pp267-275.

[12] Bennett, Charles H., Gilles Brassard, and N. David Mermin, **Quantum cryptography without Bell's theorem,** Physical Review Letters, Vol. 68, No. 5, 3 February 1992, pp 557 - 559.

[13] Bennett, Charles H., Gilles Brassards, and Jean-Marc Roberts, **Privacy amplification by public discussions,** Siam J. Comput, Vol. 17, No. 2, April 1988, pp 210 -229.

[14] Bennett, Charles H., Gilles Brassard, and Claude Crépeau, **Practical quantum oblivious transfer,** Advances in Cryptology - CRYPTO'91, Springer-Verlag (1992), pp 351 - 366.

[15] Bennett, Charles H., Gilles Brassard, and Artur Ekert, **Quantum cryptography,** Scientific American, October 1992, pp 50 - 57.

[16] Bennett, Charles H., Péter Gács, Ming Li, Paul M.B. Vitányi, and Wojciech H. Zurek, **Thermodynamics of computation and information distance,** 25-th ACM STOC '93-5/93/CA,USA ... 193 ACM 0-89791-591-7/93/0005/0021.

[17] Bennett, Charles H., **Quantum information and computation**, Physics Today, October 1995, pp 24 - 30.

[18] Bennett, C.H., G. Brassard, C. Crepeau, and U.M. Maurer, IEEE Transactions on Information Theory, 1995.

[19] Berthiaume, André and Gilles Brassard, **The quantum challenge to structural complexity theory,** prepint (7-th IEEE Structures, June, 1992), pp 132 - 137.

[20] Biham, Eli, Michel Boyer, Gilles Brassard, Jeroen van de Graaf, and Tal Mo, **Security of quantum key distribution against all collective attacks**, quant-ph/9801022.

[21] Blow, K.J., and Simon J.D. Phoenix, **On a fundamental theorem of quantum cryptography**, Journal of Modern Optics, 1993, vol. 40, no. 1, 33 - 36.

[22] Blow, K.j., Rodney Loudon, and Simon J. D. Phoenix, **Continuum fields in quantum optics,** Physical Review A, Vol. 42, No. 7, 1 October 1990, pp 4102 - 4114.

[23] Boneh, Dan, and Richard J. Lipton, **Quantum cryptanalysis of hidden linear functions**, pp 424 - 437 in "Advances in Cryptology - CRYPTO'95: Proceedings of the 15th Annual International Cryptology Conference Santa Barbara, California, USA, Agust 1995, edited by Don Coppersmith, Springer-Verlag, NY (1995).

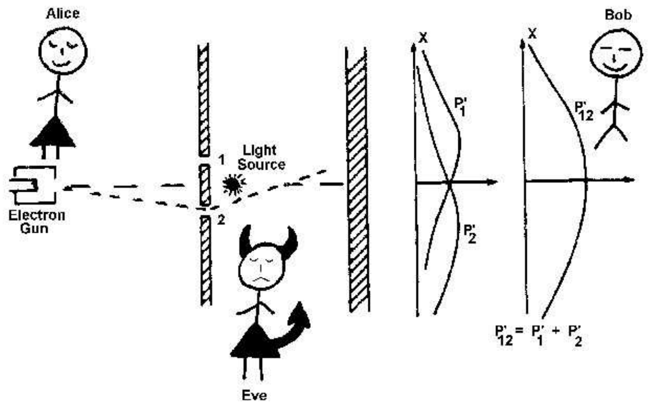


Figure 4. Young's double slit experiment when electron trajectories are observed by Eve. The second of two incompatible observables is measured.

Comparing this with our description of a classical cryptographic system, the electron gun can be thought of as the transmitter Alice. And the interference pattern P_{12} can be thought of as the message received by Bob. If however, Eve tries to eavesdrop by trying to detect through which slit each electron passes, as illustrated in Fig. 4, the interference pattern P_{12} is destroyed and replaced by the bell curve P'_{12} (which is a classical superposition of curves P'_1 and P'_2) drawn in Fig. 4, thus demonstrating the particle nature of the electron. As a result, Bob knows with certainty that Eve is eavesdropping in on his communication with Alice. Bob knows that, because of the Heisenberg uncertainty principle, both the wave and particle natures of the electron can not be simultaneously detected.

In the next sections, we describe a number of methods, i.e., **quantum cryptographic communication protocols**, that utilize the Heisenberg uncertainty principle to communicate random binary sequences (i.e., keys) with automatic eavesdrop detection. These quantum communication protocols provide a means of circumventing the "catch 22" of classical cryptographic systems. As a result, the perfect security of the Vernam cipher (i.e., one-time-pad) is an inexpensively implementable reality.

All the quantum cryptographic systems we discuss in this paper can be implemented by transmissions over fiber optic cable of individual photons, each with a single bit encoded in its quantum mechanical state space. We describe all of these systems in terms of the polarization states of a single photon. It should be noted that they could equally well be described in terms of any two-state quantum system. Examples of such a system include a spin-$\frac{1}{2}$ particle, and a two-state level atom.

The quantum cryptographic protocols discussed will of necessity use some encoding scheme (or schemes) which associates the bits 0 and 1 with distinct quantum states. We call such an association a **quantum alphabet**. Should the associated states be orthogonal, we call the encoding scheme an **orthogonal quantum alphabet**.

3 The BB84 quantum cryptographic protocol without noise

The first quantum cryptographic communication protocol, called **BB84**, was invented in 1984 by Bennett and Brassard [10][3]. This protocol has been experimentally demonstrated to work for a transmission over 30 km of fiber optic cable [101] [111] [112] [113], and also over free space for a distance of over one hundred meters[80] [67]. It is speculated, but not yet experimentally verified, that the BB84 protocol should be implementable over distances of at least 100 km.

In this section we describe the BB84 protocol in a noise free environment. In the next section, we extend the protocol to one in which noise is considered.[4]

We now describe the BB84 protocol in terms of the polarization states of a single photon. Please note that the BB84 protocol could equally well be described in terms of any other two-state quantum system.

Let $\mathcal{H}$ be the two dimensional Hilbert space whose elements representate the polarization states of a single photon. In describing BB84, we use two different orthogonal bases of $\mathcal{H}$. They are the **circular polarization basis**, which consists of the kets

$$|\curvearrowright\rangle \text{ and } |\curvearrowleft\rangle$$

[3] Quantum cryptographic protocols evolved from the earlier work of Wiesner [117].

[4] The proofs given in this and the next section are based on the assumption that Eve uses the opaque eavedropping strategy. Other eavesdropping strategies are briefly discussed in section 8 of this paper.

for **right** and **left circular polarization states**, respectively, and the **linear polarization basis** which consists of the kets

$$|\updownarrow\rangle \text{ and } |\leftrightarrow\rangle$$

for **vertical** and **horizontal linear polarization states**, respectively.

The BB84 protocol utilizes any two incompatible orthogonal quantum alphabets in the Hilbert space $\mathcal{H}$. For our description of BB84, we have selected the **circular polarization quantum alphabet** $\mathcal{A}_{\odot}$

Symbol	Bit
$\vert\curvearrowright\rangle$	1
$\vert\curvearrowleft\rangle$	0

Circular Polarization
Quantum Alphabet $\mathcal{A}_{\odot}$

and the **linear polarization quantum alphabet** $\mathcal{A}_{\boxplus}$

Symbol	Bit
$\vert\updownarrow\rangle$	1
$\vert\leftrightarrow\rangle$	0

Linear Polarization
Quantum Alphabet $\mathcal{A}_{\boxplus}$

Bennett and Brassard note that, if Alice were to use only one specific orthogonal quantum alphabet for her communication to Bob, then Eve's eavesdropping could go undetected. For Eve could intercept Alice's transmission with 100% accuracy, and then imitate Alice by retransmitting her measurements to Bob. If, for example, Alice used only the orthogonal quantum alphabet $\mathcal{A}_{\odot}$, then Eve could measure each bit of Alice's transmission with a device based on some circular polarization measurement operator such as

$$|\curvearrowright\rangle\langle\curvearrowright| \qquad \text{or} \qquad |\curvearrowleft\rangle\langle\curvearrowleft|$$

Or if, Alice used only the orthogonal quantum alphabet $\mathcal{A}_{\boxplus}$, then Eve could measure each transmitted bit with a device based on some linear polarization measurement operator such as

$$|\updownarrow\rangle\langle\updownarrow| \qquad \text{or} \qquad |\leftrightarrow\rangle\langle\leftrightarrow|$$

The above strategy used by Eve is called **opaque eavesdropping** [55]. (We will consider other and more sophisticated eavesdropping strategies later.)

To assure the detection of Eve's eavesdropping, Bennett and Brassard require Alice and Bob to communicate in two stages, the first stage over a one-way quantum communication channel from Alice to Bob, the second stage over a two-way public communication channel. (Please refer to Figure 5.)

3.1 Stage 1. Communication over a quantum channel

In the first stage, Alice is required, each time she transmits a single bit, to use randomly with equal probability one of the two orthogonal alphabets $\mathcal{A}_{\odot}$ or $\mathcal{A}_{\boxplus}$. Since no measurement operator of $\mathcal{A}_{\odot}$ is compatible with any measurement operator of $\mathcal{A}_{\boxplus}$, it follows from the Heisenberg uncertainty principle that no one, not even Bob or Eve, can receive Alice's transmission with an accuracy greater than 75%.

- Closed quantum mechanical systems transform only via unitary transformations
- Unitary transformations preserve quantum probabilities

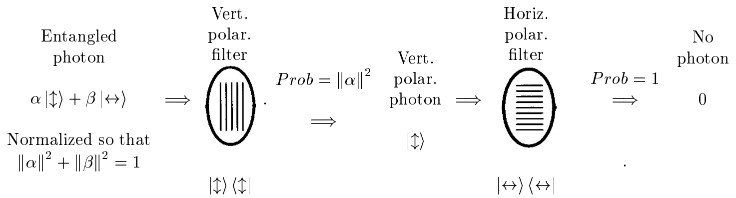
Let $|\psi(t)\rangle$ denote the state of a closed quantum mechanical system $\mathcal{S}$ as a function of time t. Then the dynamical behavior of $\mathcal{S}$ is determined by the **Schrödinger equation**

$$\frac{\partial}{\partial t}|\psi(t)\rangle = -\frac{i}{\hbar}H|\psi(t)\rangle \ ,$$

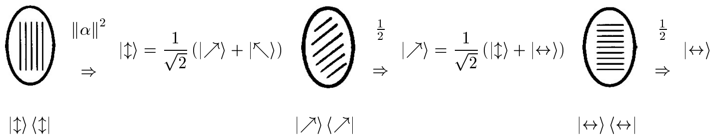
and boundary conditions, where $\hbar$ denotes Planck's constant and H denotes an observable of $\mathcal{S}$ called the **Hamiltonian**. The Hamiltonian is the quantum mechanical analog of the Hamiltonian classical mechanics. In classical physics, it is the total energy of the system.

14.9 There is much more to quantum mechanics

There is much more to quantum mechanics. For more in-depth overviews, there are many outstanding books. Among such books are [65], [104], [51], [95], [99], and many more. Some excellent insights into this subject are also given in chapter 2 of [97].



Example 9 *But if we insert a diagonally polarized filter (by 45° off the vertical) between the two polarized filters in the above example, we have:*



where the input to the first filter is $\alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle$.

14.7 A Rosetta stone for Dirac notation: Part III. Expected values

The **average value** (**expected value**) of a measurement of an observable A on a state $|\alpha\rangle$ is:

$$\langle A\rangle = \langle\alpha|\,A\,|\alpha\rangle$$

For, since

$$\sum_i |a_i\rangle\langle a_i| = 1\ ,$$

we have

$$\langle A\rangle = \langle\alpha|\,A\,|\alpha\rangle = \langle\alpha|\left(\sum_i |a_i\rangle\langle a_i|\right) A \left(\sum_j |a_j\rangle\langle a_j|\right)|\alpha\rangle = \sum_{i,j}\langle\alpha \mid a_i\rangle\langle a_i|\,A\,|a_j\rangle\langle a_j \mid \alpha\rangle$$

But on the other hand,

$$\langle a_i|\,A\,|a_j\rangle = a_j\langle a_i \mid a_j\rangle = a_i\delta_{ij}$$

Thus,

$$\langle A\rangle = \sum_i\langle\alpha \mid a_i\rangle\, a_i\,\langle a_i \mid \alpha\rangle = \sum_i a_i\,\|\langle a_i \mid \alpha\rangle\|^2$$

Hence, we have the standard expected value formula,

$$\langle A\rangle = \sum_i a_i Prob\,(\text{Observing } a_j \text{ on input } |\alpha\rangle)$$

14.8 Dynamics of closed quantum systems: Unitary transformations, the Hamiltonian, and Schrödinger's equation

An operator U on a Hilbert space $\mathcal{H}$ is **unitary** if

$$U^\dagger = U^{-1}\ .$$

Unitary operators are of central importance in quantum mechanics for many reason. We list below only two:

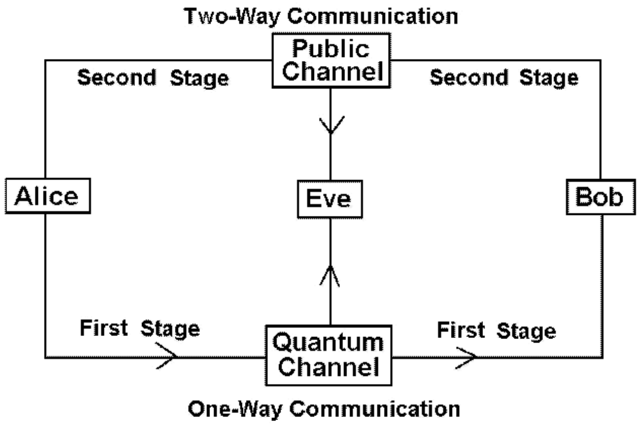


Figure 5. A quantum cryptographic communication system for securely transfering random key.

This can be seen as follows. For each bit transmitted by Alice, one can choose a measurement operator compatible with either $\mathcal{A}_\odot$ or $\mathcal{A}_\boxplus$, but not both. Because of incompatibility, there is no simultaneous measurement operator for both $\mathcal{A}_\odot$ and $\mathcal{A}_\boxplus$. Since one has no knowledge of Alice's secret choice of quantum alphabet, 50% of the time (i.e., with probability $\frac{1}{2}$) one will guess correctly, i.e., choose a measurement operator compatible with Alice's choice, and 50% of the time (i.e., with probability $\frac{1}{2}$) one will guess incorrectly. If one guesses correctly, then Alice's transmitted bit is received with probability 1. On the other hand, if one guesses incorrectly, then Alice's transmitted bit is received correctly with probability $\frac{1}{2}$. Thus in general, the probability of correctly receiving Alice's transmitted bit is

$$P = \frac{1}{2}\cdot 1 + \frac{1}{2}\cdot\frac{1}{2} = \frac{3}{4}$$

For each bit transmitted by Alice, we assume that Eve performs one of two actions, opaque eavesdropping with probability λ, $0 \le \lambda \le 1$, or no eavesdropping with probability $1-\lambda$. Thus, if $\lambda = 1$, Eve is eavesdropping on each transmitted bit; and if $\lambda = 0$, Eve is not eavesdropping at all.

Because Bob's and Eve's choice of measurement operators are stochastically independent of each other and of Alice's choice of alphabet, Eve's eavesdropping has an immediate and detectable impact on Bob's received bits. Eve's eavesdropping causes Bob's error rate to jump from $\frac{1}{4}$ to

$$\frac{1}{4}(1-\lambda) + \frac{3}{8}\lambda = \frac{1}{4} + \frac{\lambda}{8}$$

Thus, if Eve eavesdrops on every bit, i.e., if $\lambda = 1$, then Bob's error rate jumps from $\frac{1}{4}$ to $\frac{3}{8}$, a 50% increase.

3.2 Stage 2. Communication in two phases over a public channel

In stage 2, Alice and Bob communicate in two phases over a public channel to check for Eve's presence by analyzing Bob's error rate.

3.2.1 Phase 1 of Stage 2. Extraction of raw key

Phase 1 of stage 2 is dedicated to eliminating the bit locations (and hence the bits at these locations) at which error could have occurred without Eves eavesdropping. Bob begins by publicly communicating to Alice which measurement operators he used for each of the received bits. Alice then in turn publicly communicates to Bob which of his measurement operator choices were correct. After this two way communication, Alice and Bob delete the bits corresponding to the incompatible measurement choices to produce shorter sequences of bits which we call respectively **Alice's raw key** and **Bob's raw key**.

If there is no intrusion, then Alice's and Bob's raw keys will be in total agreement. However, if Eve has been at work, then corresponding bits of Alice's and Bob's raw keys will not agree with probability

$$0 \cdot (1-\lambda) + \frac{1}{4} \cdot \lambda = \frac{\lambda}{4}$$

3.2.2 Phase 2 of Stage 2. Detection of Eve's intrusion via error detection

Alice and Bob now initiate a two way conversation over the public channel to test for Eve's presence.

In the absence of noise, any discrepancy between Alice's and Bob's raw keys is proof of Eve's intrusion. So to detect Eve, Alice and Bob select a publicly agreed upon random subset of m bit locations in the raw key, and publicly compare corresponding bits, making sure to discard from raw key each bit as it is revealed.

Should at least one comparison reveal an inconsistency, then Eve's eavesdropping has been detected, in which case Alice and Bob return to stage 1 and start over. On the other hand, if no inconsistencies are uncovered, then the probability that Eve escapes detection is:

$$P_{false} = \left(1 - \frac{\lambda}{4}\right)^m$$

For example, if $\lambda = 1$ and $m = 200$, then

$$P_{false} = \left(\frac{3}{4}\right)^{200} \approx 10^{-25}$$

Thus, if P_{false} is sufficiently small, Alice and Bob agree that Eve has not eavesdropped, and accordingly adopt the remnant raw key as their **final secret key**.

4 The BB84 quantum cryptographic protocol with noise

In this section, the BB84 protocol is extended to a noisy environment. Since, in a noisy environment, Alice and Bob can not distinguish between error caused by noise and error caused by Eve's eavesdropping, they must and do adopt the assumption that all errors in raw key are caused by Eve.

As before, there are two stages to the protocol.

4.1 Stage 1. Communication over a quantum channel

This stage is exactly the same as before, except that errors are now also induced by noise.

4.2 Stage 2. Communication in four phases over a public channel

In stage 2, Alice and Bob communicate over a public channel in four phases. Phase 1 is dedicated to **raw key** extraction, phase 2 to **error estimation**, phase 3 to **reconciliation**, i.e., to **reconciled key** extraction, and phase 4 to **privacy amplification**, i.e., extraction of **final secret key**.

4.2.1 Phase 1 of Stage 2. Extraction of raw key

This stage is the same as before, except Alice and Bob also delete those bit locations at which Bob should have received but did not receive a bit. Such "non-receptions" could be caused by Eve's intrusion or by dark counts in Bob's detecting device. The location of the dark counts are, of course, communicated by Bob to Alice over the public channel.

4.2.2 Phase 2 of Stage 2. Estimation of error in raw key

Alice and Bob now use the public channel to estimate the error rate in raw key. They publicly select and agree upon a random sample of raw key, publicly compare these bits to obtain an estimate R of the error-rate. These revealed bits are discarded from raw key. If R exceeds a certain threshold R_{Max}, then it will be impossible for Alice and Bob to arrive at a common secret key. If so, Alice and Bob return to stage 1 to start over. On the other hand, If the error estimate R does not exceed R_{Max}, then Alice and Bob move onto phase 3.

14.5 Quantum measurement: General principles

In this section, A will denote a complete nondegenerate observable with eigenvalues a_i and eigenkets $|a_i\rangle$.

According to quantum measurement theory, the measurement of an observable A of a ket $|\psi\rangle$ with respect to the basis $\{|a_i\rangle\}$ produces the eigenvalue a_i with probability

$$Prob\,(\text{Value} \quad a_i \quad \text{is} \quad \text{observed}) = \|\langle a_i \mid \psi\rangle\|^2$$

and forces the state of the quantum system to become the corresponding eigenket $|a_i\rangle$.

Since quantum measurement is such a hotly debated topic among physicists, we (in self-defense) quote P.A.M. Dirac[51]:

> "A measurement always causes the (quantum mechanical) system to jump into an eigenstate of the dynamical variable that is being measured."

Thus, the above mentioned measurement of observable A of ket $|\psi\rangle$ can be diagrammatically represented as follows:

$$|\psi\rangle = \sum_i |a_i\rangle \langle a_i \mid \psi\rangle \quad \underset{Prob = \|\langle a_j \mid \psi\rangle\|^2}{\overset{\text{Meas. of } A}{\Longrightarrow}} \quad a_j\,|a_j\rangle \quad \sim \quad |a_j\rangle \quad \underset{Prob = 1}{\overset{\text{Meas. of } A}{\Longrightarrow}} \quad |a_j\rangle$$

The observable

$$|a_i\rangle \langle a_i|$$

is frequently called a **selective measurement operator** (or a **filtration**) for a_i. As mentioned earlier, it has two eigenvalues 0 and 1. 1 is a nondegenerate eigenvalue with eigenket $|a_i\rangle$, and 0 is a degenerate eigenvalue with eigenkets $\{|a_j\rangle\}_{j \neq i}$.

Thus,

$$|\psi\rangle \quad \underset{Prob = \|\langle a_i \mid \psi\rangle\|^2}{\overset{|a_i\rangle\langle a_i|}{\Longrightarrow}} \quad 1 \cdot |a_i\rangle = |a_i\rangle \ ,$$

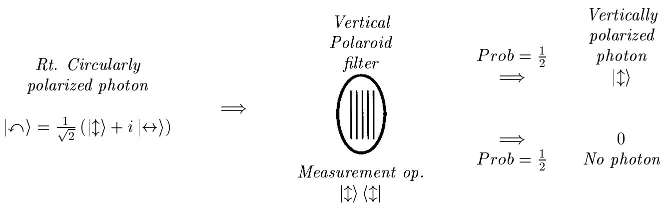
but for $j \neq i$,

$$|\psi\rangle \quad \underset{Prob = \|\langle a_j \mid \psi\rangle\|^2}{\overset{|a_i\rangle\langle a_i|}{\Longrightarrow}} \quad 0 \cdot |a_j\rangle = 0$$

14.6 Polarized light: Part III. Three examples of quantum measurement

We can now apply the above general principles of quantum measurement to polarized light. Three examples are given below:[9]

Example 7



Example 8 *A vertically polarized filter followed by a horizontally polarized filter.*

[9]The last two examples can easily be verified experimentally with at most three pair of polarized sunglasses.

Moreover, each operator $\mathcal{O}$ on $\mathcal{H}$ can be identified with an operator, also denoted by $\mathcal{O}$, on $\mathcal{H}^{\#}$ defined by

$$\langle\, label_1 \,| \longmapsto \langle\, label_1 \,|\, \mathcal{O}$$

where $\langle\, label_1 \,|\, \mathcal{O}$ is the bra defined by

$$(\langle\, label_1 \,|\, \mathcal{O})\,(|\, label_2 \rangle) = \langle\, label_1 \,|\, (\mathcal{O} \,|\, label_2 \rangle)$$

(This is sometimes called Dirac's associativity law.) Hence, the expression

$$\langle\, label_1 \,|\, \mathcal{O} \,|\, label_2 \rangle$$

is unambiguous.

Remark 4 *Please note that*

$$(\mathcal{O} \,|\, label \rangle)^{\#} = \langle label |\, \mathcal{O}^{\dagger}$$

In quantum mechanics, an **observable** is simply a **Hermitian** (also called **self-adjoint**) operator on a Hilbert space $\mathcal{H}$, i.e., an operator $\mathcal{O}$ such that

$$\mathcal{O}^{\dagger} = \mathcal{O} \ .$$

An **eigenvalue** a of an operator A is a complex number for which there is a ket $|label\rangle$ such that

$$A\,|label\rangle = a\,|label\rangle \ .$$

The ket $|label\rangle$ is called an **eigenket** of A corresponding to the eigenvalue a.

An important theorem about observables is given below:

Theorem 5 *The eigenvalues a_i of an observable A are all real numbers. Moreover, the eigenkets for distinct eigenvalues of an observable are orthogonal.*

Definition 6 *An eigenvalue is* ***degenerate*** *if there are at least two linearly independent eigenkets for that eigenvalue. Otherwise, it is* ***nondegenerate****.*

Notational Convention: If all the eigenvalues a_i of an observable A are nondegenerate, then we can and do label the eigenkets of A with the eigenvalues a_i. Thus, we can write:

$$A\,|a_i\rangle = a_i\,|a_i\rangle$$

for each eigenvalue a_i. In this paper, unless stated otherwise, we assume that the eigenvalues of observables are non-degenerate.

One exception to the above notational convention is the **measurement operator**

$$|a_i\rangle\,\langle a_i|$$

for the eigenvalue a_i, which is the outer product of ket $|a_i\rangle$ with its adjoint $\langle a_i|$. It has two eigenvalues 0 and 1. 1 is a nondegenerate eigenvalue with eigenket $|a_i\rangle$. 0 is a degenerate eigenvalue with corresponding eigenkets $\{\,|a_j\rangle\,\}_{j\neq i}$.

An observable A is said to be **complete** if its eigenkets $|a_i\rangle$ form a basis (hence, an orthonormal basis) of the Hilbert space $\mathcal{H}$. Given a complete nondegenerate observable A, then any ket $|\psi\rangle$ in $\mathcal{H}$ can be written as:

$$|\psi\rangle = \sum_i |a_i\rangle\,\langle a_i \mid \psi\rangle$$

Thus, for a complete nondegenerate observable A, we have the following operator equation which expresses the completeness of A,

$$\sum_i |a_i\rangle\,\langle a_i| = 1$$

Thus, in this notation, we have

$$A = \sum_i a_i\,|a_i\rangle\,\langle a_i|$$

4.2.3 Phase 3 of Stage 2. Extraction of reconciled key

In phase 3[5], Alice and Bob's objective is to remove all errors from what remains of raw key to produce an error free common key, called **reconciled key**. This phase is of course called **reconciliation**, and takes place in two steps [6] .

In step 1, Alice and Bob publicly agree upon a random permutation, and apply it to what remains of their respective raw keys. Next Alice and Bob partition the remnant raw key into blocks of length ℓ, where the length ℓ is chosen so that blocks of this length are unlikely to contain more than one error. For each of these blocks, Alice and Bob publicly compare overall parity checks, making sure each time to discard the last bit of the compared block. Each time a overall parity check does not agree, Alice and Bob initiate a binary search for the error, i.e., bisecting the block into two subblocks, publicly comparing the parities for each of these subblocks, discarding the right most bit of each subblock. They continue their bisective search on the subblock for which their parities are not in agreement. This bisective search continues until the erroneous bit is located and deleted. They then continue to the next ℓ-block.

Step 1 is repeated, i.e., a random permutation is chosen, remnant raw key is partitioned into blocks of length ℓ, parities are compared, etc. This is done until it becomes inefficient to continue in this fashion.

Alice and Bob then move to step 2 by using a more refined reconciliation procedure. They publicly select randomly chosen subsets of remnant raw key, publicly compare parities, each time discarding an agreed upon bit from their chosen key sample. If a parity should not agree, they employ the binary search strategy of step 1 to locate and delete the error.

Finally, when, for some fixed number N of consecutive repetitions of step 2, no error is found, Alice and Bob assume that to a very high probability, the remnant raw key is without error. Alice and Bob now rename the remnant raw key **reconciled key**, and move on to the final and last phase of their communication.

4.2.4 Phase 4 of Stage 2. Privacy amplification, i.e., extraction of final secret key

Alice and Bob now have a common reconciled key which they know is only partially secret from Eve. They now begin the process of **privacy amplification**, which is the extraction of a secret key from a partially secret one [6] [13].

Based on their error estimate R, Alice and Bob obtain an upper bound k of the number of bits known by Eve of their n bits of reconciled key. Let s be a security parameter that Alice and Bob adjust as desired. They then publicly select $n - k - s$ random subsets of reconciled key, without revealing their contents, and without revealing their parities. The undisclosed parities become the common **final secret key**. It can be shown that Eve's average information about the final secret key is less than $2^{-s}/\ln 2$ bits.

4.3 "Priming the pump" to start authentication

Unfortunately, there is no known way to initiate authentication without initially exchanging secret key over a secure communication channel. So, quantum protocols have not entirely overcome the "catch 22" of classical cryptography. However, this secret key exchange for authentication need only be done once. Thereafter, a portion of the secure key communicated via a quantum protocol can be used for authentication.

5 The B92 quantum cryptographic protocol

As with the BB84 quantum protocol, the B92 protocol [7] can be described in terms of any quantum system represented by a two dimensional Hilbert space. For our description, we choose the two dimensional Hilbert space $\mathcal{H}$ representing the polarization states of a single photon.

B92 can be implemented in terms of any non-orthogonal basis. We choose as our non-orthogonal basis the kets

$$|\theta\rangle \quad \text{and} \quad |\overline{\theta}\rangle\,,$$

where $|\theta\rangle$ and $|\overline{\theta}\rangle$ denote respectively the kets representing the polarization state of a photon linearly polarized at an angle θ and an angle $-\theta$ with respect to the vertical, where $0 < \theta < \pi/4$.

[5] The procedure given in Phase 3 Stage 2 is only one of many possible procedures. In fact, there are now much more efficient procedures than the procedure described below.

Unlike BB84 which requires two orthogonal quantum alphabets, B92 requires only a single non-orthogonal quantum alphabet. We choose the non-orthogonal quantum alphabet $\mathcal{A}_\theta$:

Symbol	Bit
$\lvert\theta\rangle$	1
$\lvert\overline{\theta}\rangle$	0

Linear Polarization
Quantum Alphabet $\mathcal{A}_\theta$

As in BB84, Alice and Bob communicate in two stages, the first over a one-way quantum channel, the second over a two-way public channel.

5.1 Stage 1. Communication over a quantum channel

Alice uses the quantum alphabet $\mathcal{A}_\theta$ to send her random binary sequence to Bob. Since $|\theta\rangle$ and $|\overline{\theta}\rangle$ are not orthogonal, there is no one experiment that will unambiguously distinguish between these two polarization states.

Bob can use one of many possible measurement strategies. Bennett [7] suggests the measurements be based on the two incompatible experiments corresponding to the projection operators

$$P_{\neg\theta} = 1 - |\theta\rangle\langle\theta| \quad \text{and} \quad P_{\neg\overline{\theta}} = 1 - |\overline{\theta}\rangle\langle\overline{\theta}|$$

In this case, Bob either correctly detects Alice's transmitted bit, or an ambiguous result, i.e., an **erasure**, denoted by "?". Assuming that Alice transmits 0's and 1's at random with equal probability and that, for each incoming bit, Bob at random with equal probability chooses to base his experiment on either of the incompatible operators $P_{\neg\theta}$ or $P_{\neg\overline{\theta}}$, then the probability of Bob's correctly receiving Alice's transmission is

$$\frac{1 - \left\|\langle\theta \mid \overline{\theta}\rangle\right\|^2}{2}$$

and the probability of receiving an erasure is

$$\frac{1 + \left\|\langle\theta \mid \overline{\theta}\rangle\right\|^2}{2}$$

where

$$\left\|\langle\theta \mid \overline{\theta}\rangle\right\| = \cos(2\theta)$$

and where $0 < \theta < \pi/4$. Thus, Bob receives more than 50% erasures.

On the other hand, Ekert et al [55] suggest a more efficient measurement process for Bob. They suggest that Bob base his experiments on the **positive operator valued measure** (**POVM**) [36] [99] consisting of the operators

$$A_\theta = \frac{P_{\neg\theta}}{1 + \left\|\langle\theta \mid \overline{\theta}\rangle\right\|}, \quad A_{\overline{\theta}} = \frac{P_{\neg\overline{\theta}}}{1 + \left\|\langle\theta \mid \overline{\theta}\rangle\right\|}, \text{ and } \quad A_? = 1 - A_\theta - A_{\overline{\theta}}$$

With this more efficient detection method, the probability of an inconclusive result is now

$$\left\|\langle\theta \mid \overline{\theta}\rangle\right\| = \cos(2\theta)$$

where again $0 < \theta < \pi/4$.

5.1.1 Stage 2. Communication in four phases over a public channel

Stage2 for the B92 protocol is the same as that for the BB84 protocol except for phase 1.

In phase 1 of stage 2, Bob publicly informs Alice as to which time slots he received non-erasures. The bits in these time slots become Alice's and Bob's raw keys.

Eve's presence is detected by an unusual error rate in Bob's raw key. It is also possible to detect Eve's presence by an unusual erasure rate for Bob. However, Ekert et al [55] do point out that Eve can choose eavesdropping strategies which have no effect on the erasure rate, and hence, can only be detected by unusual error rates in Bob's raw key[6].

[6]This is true for all 2-state protocols. On the other hand, for n-state protocols with $n > 2$, Eve's presence is always detectable from rejected key. See section 7 of this paper.

Convention: Since a quantum mechanical state is represented by a state ket up to a multiplicative constant, we will unless stated otherwise, choose those kets $|\alpha\rangle$ which are unit normal, i.e., such that

$$\langle\alpha \mid \alpha\rangle = 1 \Longleftrightarrow \left\| |\alpha\rangle \right\| = 1$$

The polarization states of a photon are represented as state kets in a two dimensional Hilbert space $\mathcal{H}$. One orthonormal basis of $\mathcal{H}$ consists of the kets

$$|\curvearrowleft\rangle \text{ and } |\curvearrowright\rangle$$

which represent respectively the quantum mechanical states of left- and right-circularly polarized photons. Another orthonormal basis consists of the kets

$$|\updownarrow\rangle \text{ and } |\leftrightarrow\rangle$$

representing respectively vertically and horizontally linearly polarized photons. And yet another orthonormal basis consists of the kets

$$|\nearrow\rangle \text{ and } |\searrow\rangle$$

for linearly polarized photons at the angles $\theta = \pi/4$ and $\theta = -\pi/4$ off the vertical, respectively.

These orthonormal bases are related as follows:

$$\begin{cases} |\nearrow\rangle &= \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle + |\leftrightarrow\rangle\right) \\ |\searrow\rangle &= \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle - |\leftrightarrow\rangle\right) \end{cases} \qquad \begin{cases} |\nearrow\rangle &= \frac{1+i}{2}|\curvearrowright\rangle + \frac{1-i}{2}|\curvearrowleft\rangle \\ |\searrow\rangle &= \frac{1-i}{2}|\curvearrowright\rangle + \frac{1+i}{2}|\curvearrowleft\rangle \end{cases}$$

$$\begin{cases} |\updownarrow\rangle &= \frac{1}{\sqrt{2}}\left(|\nearrow\rangle + |\nwarrow\rangle\right) \\ |\leftrightarrow\rangle &= \frac{1}{\sqrt{2}}\left(|\nearrow\rangle - |\nwarrow\rangle\right) \end{cases} \qquad \begin{cases} |\updownarrow\rangle &= \frac{1}{\sqrt{2}}\left(|\curvearrowright\rangle + |\curvearrowleft\rangle\right) \\ |\leftrightarrow\rangle &= \frac{i}{\sqrt{2}}\left(|\curvearrowright\rangle - |\curvearrowleft\rangle\right) \end{cases}$$

$$\begin{cases} |\curvearrowright\rangle &= \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle - i\,|\leftrightarrow\rangle\right) \\ |\curvearrowleft\rangle &= \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle + i\,|\leftrightarrow\rangle\right) \end{cases} \qquad \begin{cases} |\curvearrowright\rangle &= \frac{1-i}{2}|\nearrow\rangle + \frac{1+i}{2}|\nwarrow\rangle \\ |\curvearrowleft\rangle &= \frac{1+i}{2}|\nearrow\rangle + \frac{1-i}{2}|\nwarrow\rangle \end{cases}$$

The bracket products of the various polarization kets are given in the table below:

	$\lvert\updownarrow\rangle$	$\lvert\leftrightarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\curvearrowright\rangle$	$\lvert\curvearrowleft\rangle$
$\langle\updownarrow\rvert$	1	0	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$
$\langle\leftrightarrow\rvert$	0	1	$\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}}$	$-\frac{i}{\sqrt{2}}$	$\frac{i}{\sqrt{2}}$
$\langle\nearrow\rvert$	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$	1	0	$\frac{1+i}{2}$	$\frac{1-i}{2}$
$\langle\nwarrow\rvert$	$\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}}$	0	1	$\frac{1-i}{2}$	$\frac{1+i}{2}$
$\langle\curvearrowright\rvert$	$\frac{1}{\sqrt{2}}$	$\frac{i}{\sqrt{2}}$	$\frac{1-i}{2}$	$\frac{1+i}{2}$	1	0
$\langle\curvearrowleft\rvert$	$\frac{1}{\sqrt{2}}$	$-\frac{i}{\sqrt{2}}$	$\frac{1+i}{2}$	$\frac{1-i}{2}$	0	1

14.4 A Rosetta stone for Dirac notation: Part II. Operators

An **(linear) operator** or **transformation** $\mathcal{O}$ on a ket space $\mathcal{H}$ is a Hilbert space morphism of $\mathcal{H}$ into $\mathcal{H}$, i.e., is an element of

$$Hom_{\mathbb{C}}(\mathcal{H}, \mathcal{H})$$

The **adjoint** $\mathcal{O}^\dagger$ of an operator $\mathcal{O}$ is that operator such that

$$\left(\mathcal{O}^\dagger \mid label_1\,\rangle, \mid label_2\,\rangle\right) = \left(\mid label_1\,\rangle, \mathcal{O} \mid label_2\,\rangle\right)$$

for all kets $|\,label_1\,\rangle$ and $|\,label_2\,\rangle$.

In like manner, an (linear) operator or transformation on a bra space $\mathcal{H}^\#$ is an element of

$$Hom_{\mathbb{C}}\left(\mathcal{H}^\#, \mathcal{H}^\#\right)$$

The elements of $\mathcal{H}^\#$ will be called **bra vectors**, **state bras**, or simply **bras**. They will be denoted as:

$$\langle\, label \,|$$

where once again '*label*' denotes some label.

Also please note that the complex number

$$\langle\, label_1 \,|\, (|\, label_2 \,\rangle)$$

will simply be denoted by

$$\langle\, label_1 \,\mid\, label_2 \,\rangle$$

and will be called the **bra-(c)-ket** product of the bra $\langle\, label_1 \,|$ and the ket $|\, label_2 \,\rangle$.

There is a monomorphism (which is an isomorphism if the underlying Hilbert space is finite dimensional)

$$\mathcal{H} \xrightarrow{\#} \mathcal{H}^\#$$

defined by

$$|\, label \,\rangle \longmapsto (\,|\, label \,\rangle\,, -)$$

The bra $(\,|\, label \,\rangle\,, -)$ is denoted by $\langle\, label \,|$.

Hence,

$$\langle\, label_1 \,\mid\, label_2 \,\rangle = (|\, label_1 \,\rangle\,, |\, label_2 \,\rangle)$$

Remark 3 *Please note that* $(\lambda\,|\, label \,\rangle)^\# = \lambda^* \langle label|$.

The **tensor product**[8] $\mathcal{H} \otimes \mathcal{K}$ of two Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$ is simply the "simplest" Hilbert space such that

1) $(h_1 + h_2) \otimes k = h_1 \otimes k + h_2 \otimes k$, for all h, h_1, $h_2 \in \mathcal{H}$ and for all k, k_1, $k_2 \in \mathcal{K}$, and

2) $h \otimes (k_1 + k_2) = h \otimes k_1 + h \otimes k_2$ for all h, h_1, $h_2 \in \mathcal{H}$ and for all k, k_1, $k_2 \in \mathcal{K}$.

It immediately follows that

3) $\lambda\,(h \otimes k) \equiv (\lambda h) \otimes k = h \otimes (\lambda k)$ for all $\lambda \in \mathbb{C}$, $h \in \mathcal{H}$, $k \in \mathcal{K}$.

Finally, if $|\, label_1 \,\rangle$ and $|\, label_2 \,\rangle$ are kets respectively in Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, then their tensor product will be written in any one of the following three ways:

$$|\, label_1 \,\rangle \otimes |\, label_2 \,\rangle$$

$$|\, label_1 \,\rangle\, |\, label_2 \,\rangle$$

$$|\, label_1 \,,\, label_2 \,\rangle$$

14.3 Polarized light: Part II. The quantum mechanical perspective

The states of a quantum mechanical system are represented by state kets in a Hilbert space $\mathcal{H}$. Two kets $|\alpha\rangle$ and $|\beta\rangle$ represent the same quantum mechanical state if they differ by a non-zero multiplicative constant. I.e., $|\alpha\rangle$ and $|\beta\rangle$ represent the same quantum mechanical state if there exists a non-zero $\lambda \in \mathbb{C}$ such that

$$|\alpha\rangle = \lambda\, |\beta\rangle$$

Hence, the quantum mechanical states are the elements of the manifold

$$\mathcal{H}/\tilde{} = \mathbb{C}P^n$$

where n denotes the dimension of $\mathcal{H}$, and $\mathbb{C}P^n$ denotes complex projective space.

[8] Readers well versed in homological algebra will recognize this informal definition as a slightly disguised version of the more rigorous universal definition of the tensor product. For more details, please refer to [37], or any other standard reference on homological algebra.

6 EPR quantum cryptographic protocols

Ekert in [60] has devised a quantum protocol based on the properties of quantum-correlated particles.

Einstein, Podolsky, and Rosen (EPR) in the their famous 1935 paper [64] challenged the foundations of quantum mechanics by pointing out a "paradox." There exist spatially separated pairs of particles, henceforth called **EPR pairs**, whose states are correlated in such a way that the measurement of a chosen observable A of one automatically determines the result of the measurement of A of the other. Since EPR pairs can be pairs of particles separated at great distances, this leads to what appears to be a paradoxical "action at a distance."

For example, it is possible to create a pair of photons (each of which we label below with the subscripts 1 and 2, respectively) with correlated linear polarizations. An example of such an entangled state is given by

$$|\Omega_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1 \left|\frac{\pi}{2}\right\rangle_2 - \left|\frac{\pi}{2}\right\rangle_1 |0\rangle_2\right)$$

where the notation $|\theta\rangle$ has been defined in the previous section. Thus, if one photon is measured to be in the vertical linear polarization state $|0\rangle$, the other, when measured, will be found to be in the horizontal linear polarization state $|\pi/2\rangle$, and vice versa.

Einstein et al [64] then state that such quantum correlation phenomena could be a strong indication that quantum mechanics is incomplete, and that there exist "hidden variables," inaccessible to experiments, which explain such "action at a distance."

In 1964, Bell [4] gave a means for actually testing for **locally hidden variable** (**LHV**) theories. He proved that all such LHV theories must satisfy the **Bell inequality**. Quantum mechanics has been shown to violate the inequality.

The **EPR quantum protocol** is a 3-state protocol that uses Bell's inequality to detect the presence or absence of Eve as a hidden variable. Following the theme of this paper, we now describe this protocol in terms of the polarization states of an EPR photon pair. As the three possible polarization states of our EPR pair, we choose

$$|\Omega_0\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle_1 \left|\tfrac{3\pi}{6}\right\rangle_2 - \left|\tfrac{3\pi}{6}\right\rangle_1 |0\rangle_2\right).$$

$$|\Omega_1\rangle = \tfrac{1}{\sqrt{2}}\left(\left|\tfrac{\pi}{6}\right\rangle_1 \left|\tfrac{4\pi}{6}\right\rangle_2 - \left|\tfrac{4\pi}{6}\right\rangle_1 \left|\tfrac{\pi}{6}\right\rangle_2\right), \text{ and}$$

$$|\Omega_2\rangle = \tfrac{1}{\sqrt{2}}\left(\left|\tfrac{2\pi}{6}\right\rangle_1 \left|\tfrac{5\pi}{6}\right\rangle_2 - \left|\tfrac{5\pi}{6}\right\rangle_1 \left|\tfrac{2\pi}{6}\right\rangle_2\right)$$

For each of these states, we choose the following corresponding mutually non-orthogonal alphabets $\mathcal{A}_0$, $\mathcal{A}_1$,and $\mathcal{A}_2$, given by the following tables:

Symbol	Bit
$\lvert 0\rangle$	0
$\lvert \frac{3\pi}{6}\rangle$	1

Linear Polarization
Quantum Alphabet $\mathcal{A}_0$

Symbol	Bit
$\lvert \frac{\pi}{6}\rangle$	0
$\lvert \frac{4\pi}{6}\rangle$	1

Linear Polarization
Quantum Alphabet $\mathcal{A}_1$

Symbol	Bit
$\lvert \frac{2\pi}{6}\rangle$	0
$\lvert \frac{5\pi}{6}\rangle$	1

Linear Polarization
Quantum Alphabet $\mathcal{A}_2$

The corresponding measurement operators chosen for these alphabets are respectively

$$\mathcal{M}_0 = |0\rangle\langle 0|\,, \quad \mathcal{M}_1 = \left|\frac{\pi}{6}\right\rangle\left\langle\frac{\pi}{6}\right|, \text{ and } \mathcal{M}_2 = \left|\frac{2\pi}{6}\right\rangle\left\langle\frac{2\pi}{6}\right|$$

As with the BB84 and B92 , there are two stages to the EPR protocol, the first stage over a quantum channel, the second over a public channel.

6.1 Stage 1. Communication over a quantum channel

For each time slot, a state $|\Omega_j\rangle$ is randomly selected with equal probability from the set of states $\{|\Omega_0\rangle\,, |\Omega_1\rangle\,, |\Omega_2\rangle\}$. Than an EPR pair is created in the selected state $|\Omega_j\rangle$. One photon of the constructed EPR pair is sent to Alice, the other to Bob. Alice and Bob at random with equal probability separately and independently select one of the three measurement operators $\mathcal{M}_0$, $\mathcal{M}_1$, and $\mathcal{M}_2$, and accordingly measure their respective photons. Alice records her measured bit. On the other hand, Bob records the complement of his measured bit. This procedure is repeated for as many time slots as needed.

6.2 Stage 2. Communication over a public channel

In stage 2, Alice and Bob communicate over a public channel.

6.2.1 Phase 1 of Stage2. Separation of key into raw and rejected keys

In phase 1 of stage 2, Alice and Bob carry on a discussion over a public channel to determine those bit slots at which they used the same measurement operators. They each then separate their respective bit sequences into two subsequences. One subsequence, called **raw key**, consists of those bit slots at which they used the same measurement operators. The other subsequence, called **rejected key**, consists of all the remaining bit slots.

6.2.2 Phase 2 of Stage 2. Detection of Eve's presence with Bell's inequality applied to rejected key

Unlike the BB84 and B92 protocols, the EPR protocol, instead of discarding rejected key, actually uses it to detect Eve's presence. Alice and Bob now carry on a discussion over a public channel comparing their respective rejected keys to determine whether or not Bell's inequality is satisfied. If it is, Eve's presence is detected. If not, then Eve is absent.

For the EPR protocol, Bell's inequality can be written as follows. Let $P(\neq| i,j)$ denote the probability that two corresponding bits of Alice's and Bob's rejected keys do not match given that the measurement operators chosen by Alice and Bob are respectively either $\mathcal{M}_i$ and $\mathcal{M}_j$ or $\mathcal{M}_j$ and $\mathcal{M}_i$. Let $P(=| i,j) = 1 - P(\neq| i,j)$. Let

$$\Delta(i,j) = P(\neq| i,j) - P(=| i,j)$$

Finally, let

$$\beta = 1 + \Delta(1,2) - |\Delta(0,1) - \Delta(0,2)|$$

Then Bell's inequality in this case reduces to

$$\beta \geq 0$$

Moreover, for quantum mechanics (i.e., no hidden variables)

$$\beta = -\frac{1}{2}$$

which is a clear violation of Bell's inequality.

6.2.3 Phase 3 of Stage 2. Reconciliation

In the presence of noise, the remaining phase of the EPR protocol is reconciliation, as described in the BB84 and B92 protocols.

7 Other protocols

It is not possible to cover all possible quantum protocols in this paper. There is the EPR protocol with a single particle. There is also a 2-state EPR implementation of the BB84 protocol. For details, see [12] [46]. For various **multiple state** and **rejected data protocols**, see [21].

8 Eavesdropping strategies and counter measures

There are many eavesdropping strategies available to Eve. (See for example [55],[24].) We list only a few.

14 Appendix C. Part of a Rosetta stone for quantum mechanics.

This appendix is intended for readers unfamiliar with quantum mechanics. It's purpose is to provide those readers with enough background in quantum mechanics to understand a substantial portion of this paper. Because of space limitations, this appendix is of necessity far from a complete overview of the subject.

14.1 Polarized light: Part I. The classical perspective

Light waves in the vacuum are transverse electromagnetic (EM) waves with both electric and magnetic field vectors perpendicular to the direction of propagation and also to each other. (See figure 6.)

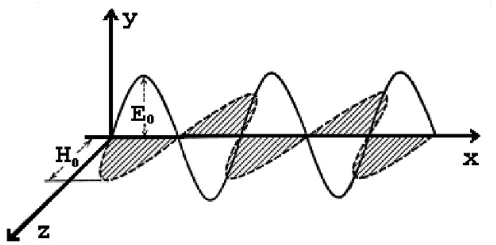


Figure 6. A linearly polarized electromagnetic wave.

If the electric field vector is always parallel to a fixed line, then the EM wave is said to be **linearly polarized**. If the electric field vector rotates about the direction of propagation forming a right-(left-)handed screw, it is said to be **right** (**left**) **elliptically polarized**. If the rotating electric field vector inscribes a circle, the EM wave is said to be right-or left-**circularly polarized**.

14.2 A Rosetta stone for Dirac notation: Part I. Bras, kets, and bra-(c)-kets

A **Hilbert space** $\mathcal{H}$ is a vector space over the complex numbers $\mathbb{C}$ with a complex valued inner product

$$(-,-) : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$$

which is complete with respect to the norm

$$\|u\| = \sqrt{(u,u)}$$

induced by the inner product.

Remark 1 *By a complex valued inner product, we mean a map*

$$(-,-) : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$$

from $\mathcal{H} \times \mathcal{H}$ into the complex numbers $\mathbb{C}$ such that:

1) $(u,u) = 0$ *if and only if* $u = 0$

2) $(u,v) = (v,u)^*$

3) $(u, v+w) = (u,v) + (u,w)$

4) $(u, \lambda v) = \lambda(u,v)$

where '' denotes the complex conjugate.*

Remark 2 *(Please note that $(\lambda u, v) = \lambda^*(u,v)$.)*

The elements of $\mathcal{H}$ will be called **ket vectors**, **state kets**, or simply **kets**. They will be denoted as:

$$|\,label\,\rangle$$

where '*label*' denotes some label.

Let $\mathcal{H}^{\#}$ denote the Hilbert space of all Hilbert space morphisms of $\mathcal{H}$ into the Hilbert space of all complex numbers $\mathbb{C}$, i.e.,

$$\mathcal{H}^{\#} = Hom_{\mathbb{C}}(\mathcal{H}, \mathbb{C}) .$$

13 Appendix B. Proof that an undetectable eavesdropper can obtain no information from the B92 protocol

In this appendix we prove that an undetectable eavesdropper for the B92 protocol obtains no information whatsoever. The proof is taken from [12].

Let $|a\rangle$ and $|b\rangle$ denote the two non-orthogonal states used in the B92 protocol[7]. Thus,

$$\langle a \mid b\rangle \neq 0$$

Let U be the unitary transformation performed by Eve's detection probe, which we assume is initially in state $|\Psi\rangle$.

Since Eve's probe is undetectable, we have

$$|\Psi\rangle\,|a\rangle \mapsto U\,|\Psi\rangle\,|a\rangle = |\Psi'\rangle\,|a\rangle$$

$$|\Psi\rangle\,|b\rangle \mapsto U\,|\Psi\rangle\,|b\rangle = |\Psi''\rangle\,|b\rangle$$

where $|\Psi'\rangle$ and $|\Psi''\rangle$ denote the states of Eve's prober after the detection of $|a\rangle$ and $|b\rangle$ respectively. Please note that, since Eve is undetectable, her probe has no effect on the states $|a\rangle$ and $|b\rangle$. So $|a\rangle$ appears on both sides of the first equation, and $|b\rangle$ appears on both sides of the second equation.

Thus,

$$\langle a|\,\langle\Psi|\,U^{\dagger}U\,|\Psi\rangle\,|b\rangle = \langle a|\,\langle\Psi \mid \Psi\rangle\,|b\rangle = \langle a \mid b\rangle\,,$$

because of the unitarity of U and because $\langle\Psi \mid \Psi\rangle = 1$. On the other hand,

$$\langle a|\,\langle\Psi' \mid \Psi''\rangle\,|b\rangle = \langle\Psi' \mid \Psi''\rangle\,\langle a \mid b\rangle\,.$$

As a result, we have the equation

$$\langle a \mid b\rangle = \langle\Psi' \mid \Psi''\rangle\,\langle a \mid b\rangle$$

But $\langle a \mid b\rangle \neq 0$ implies that $\langle\Psi' \mid \Psi''\rangle = 1$. Since $|\Psi'\rangle$ and $|\Psi''\rangle$ are normalized, this implies that $|\Psi'\rangle = |\Psi''\rangle$. It follows that Eve's probe is in the same state no matter which of the states $|a\rangle$ and $|b\rangle$ is received. Thus, Eve obtains no information whatsoever.

[7] In section 6 of this paper we denoted these states by $|\theta\rangle$ and $\left|\overline{\theta}\right\rangle$.

8.1 Opaque eavesdropping

For this strategy, Eve intercepts Alice's message, and then masquerades as Alice by sending her received message on to Bob. Opaque eavesdropping has already been discussed in sections 4 and 5 of this paper. For more information, the reader is referred to [55].

8.2 Translucent eavesdropping without entanglement

For this strategy, Eve makes the information carrier interact unitarily with her probe, and then lets it proceed on to Bob in a slightly modified state. In the case of the B92 protocol, Eve's detection probe with initial state $|\Psi\rangle$ would perform a unitary transformation U of the form

$$\begin{cases} |\theta\rangle\,|\Psi\rangle \mapsto U\,|\theta\rangle\,|\Psi\rangle = |\theta'\rangle\,|\Psi_\theta\rangle \\ \\ \left|\overline{\theta}\right\rangle|\Psi\rangle \mapsto U\left|\overline{\theta}\right\rangle|\Psi\rangle = \left|\overline{\theta}'\right\rangle\left|\Psi_{\overline{\theta}}\right\rangle \end{cases}$$

where $|\theta'\rangle$ and $\left|\overline{\theta}'\right\rangle$ denote the slightly changed states received by Bob after the action of the probe, and where $|\Psi_\theta\rangle$ and $\left|\Psi_{\overline{\theta}}\right\rangle$ denote the states of the probe after the transformation.. We refer the reader to [55] for an in depth analysis of this eavesdropping strategy.

8.3 Translucent eavesdropping with entanglement

For this strategy, Eve entangles the state of her probe and the carrier, and then she sends the carrier on to Bob. In the case of the B92 protocol, Eve's detection probe with initial state $|\Psi\rangle$ would perform a unitary transformation U of the form

$$\begin{cases} |\theta\rangle\,|\Psi\rangle \mapsto U\,|\theta\rangle\,|\Psi\rangle = a\,|\theta\rangle\,|\Psi_\theta\rangle + b\left|\overline{\theta}\right\rangle\left|\Psi_{\overline{\theta}}\right\rangle \\ \\ \left|\overline{\theta}\right\rangle|\Psi\rangle \mapsto U\left|\overline{\theta}\right\rangle|\Psi\rangle = b\,|\theta\rangle\,|\Psi_\theta\rangle + a\left|\overline{\theta}\right\rangle\left|\Psi_{\overline{\theta}}\right\rangle \end{cases}$$

We refer the reader to [55], [24] for an in depth analysis of this eavesdropping strategy.

8.4 Countermeasures to Eve's eavesdropping strategies

As far as the author has been able to determine, all quantum intrusion detection algorithms in the open literature depend on some assumption as to which eavesdropping strategy is chosen by Eve. It is important that eavesdropping algorithms be developed that detect Eve's intrusion no matter which eavesdropping strategy she chooses to use. (For some insight in intrusion detection algorithms, the reader is referred to [55],[24].)

9 Conclusion

It is not easy to emphasize how dramatic an impact the application of quantum mechanics has had and will have on cryptographic communication systems. From the perspective of defensive cryptography, it is now within the realm of possibility to build practical cryptographic systems which check for, detect, and prevent unauthorized intrusion. Quantum mechanics provides an intrusion detection mechanism never thought possible within the world of classical cryptography. Most importantly, the feasibility of these methods has been experimentally verified in a laboratory setting.

Moreover, from the perspective of offensive cryptography, the application of quantum mechanics to computation also holds forth the promise of a dramatic increase of computational parallelism for cryptanalytic attacks. Shor's quantum factoring algorithm [107] [57] is just one example of such potential. However, unlike quantum protocols, quantum computational parallelism has yet to be fully verified in a laboratory setting.

Much remains to be done before quantum cryptography is a truly practical and useful tool for cryptographic communication. We list below some of the areas in need of development:

- Quantum protocols need to be extended to a computer network setting. (See [102] and [115].)
- More sophisticated error correction and detection techniques need to be implemented in quantum protocols. (See [6], [13], and [18].)

- There is a need for greater understanding of intrusion detection in the presence of noise. The no cloning theorem of Appendix A of this paper and the "no detection implies no information" theorem of Appendix B of this paper simply do not provide a complete picture. (See [55].)
- There is a need for better intrusion detection algorithms. As far as the author has been able to determine, all quantum intrusion detection algorithms in the open literature depend on some assumption as to which eavesdropping strategy is chosen by Eve. It is important that eavesdropping algorithms be developed that detect Eve's intrusion no matter which eavesdropping strategy she uses. (See [55].)

10 Acknowledgment

I would like to thank Howard Brandt for his helpful discussions, and the referees for their helpful suggestions. Finally I would like to thank Alan Sherman for his encouragement to publish this paper.

11 Addendum

Quantum cryptography has continued its rapid pace of development since this paper was written. There is the recent experimental work found in [93], [94]. Progress has been made in correcting errors received from noisy channels [32], [33], [62], [63]. A number of protocols, in particular, the quantum bit commitment protocol, have been shown to be insecure [83], [84], [86]. There has been progress in the development of multi-user quantum cryptography [116]. The security of quantum cryptography against collective key attacks has been studied [20]. There have been at least two independent claims of the proof of ultimate security of quantum cryptography, i.e., security against all possible attacks [85], [87], [88], [89]. Finally, although tangentially related to this paper, it should be mentioned that a new quantum algorithm for searching databases has been developed [71], [72], [73].

12 Appendix A. The no cloning theorem

In this appendix, we prove that there can be no device that produces exact replicas or copies of a quantum system. If such a "quantum copier" existed, then Eve could eavesdrop without detection. This proof is taken from [99]. It is an amazingly simple application of the linearity of quantum mechanics. (See also [119] for a proof using the creation operators of quantum electrodynamics.)

Let us assume that there exists a **quantum replicator** initially in state $|\Psi\rangle$ which duplicates quantum systems via a unitary transformation U.

Let $|u\rangle$ and $|v\rangle$ be two arbitrary states such that

$$0 < \| \langle u \mid v \rangle \| < 1 .$$

Then the application of the quantum replicator to $|u\rangle$ and $|v\rangle$ yields

$$|\Psi\rangle |u\rangle \mapsto U |\Psi\rangle |u\rangle = |\Psi'\rangle |u\rangle |u\rangle$$

$$|\Psi\rangle |v\rangle \mapsto U |\Psi\rangle |u\rangle = |\Psi''\rangle |v\rangle |v\rangle$$

where $|\Psi'\rangle$ and $|\Psi''\rangle$ denote the states of the quantum replicator after the two respective duplications.

Thus,

$$\langle u| \langle \Psi| U^{\dagger} U |\Psi\rangle |v\rangle = \langle u| \langle \Psi \mid \Psi\rangle |v\rangle = \langle u \mid v\rangle ,$$

because of the unitarity of U and because $\langle \Psi \mid \Psi \rangle = 1$. On the other hand,

$$\langle u| \langle u| \langle \Psi' \mid \Psi''\rangle |v\rangle |v\rangle = \langle \Psi' \mid \Psi''\rangle \langle u \mid v\rangle^2 .$$

As a result, we have the equation

$$\langle u \mid v\rangle = \langle \Psi' \mid \Psi''\rangle \langle u \mid v\rangle^2$$

But this equation cannot be satisfied since $\| \langle \Psi' \mid \Psi'' \rangle \| \leq 1$ and $|u\rangle$ and $|v\rangle$ were chosen so that $0 < \| \langle u \mid v\rangle \| < 1$.

Hence, a quantum replicator cannot exist.