3 Physical limitations to computations

Physics imposes a number of limitations to the power of computation. These are different from mathematical limitations (e.g. complexity classes) mentioned in Sec. 2.5 and deal with the construction of a computational device. These limitations arise on all levels and relate to the performance of all computational steps, such as the storage of information, logical operations, or transfer of information between different parts of the computer. While some of these issues (such as the speed of light as a limit for information transfer) are quite obvious, others have only recently been discovered.

Fundamental limitations – A number of limitations derive from the actual hardware used to perform the computation, such as the CMOS technology used in today's computers. In this section, however, we would like to explore limitations that are more fundamental, independent of the current implementation. Computations are always done with devices (or brains) that obey physical laws. Correspondingly, physical laws must limit the power of these devices. Some of the issues that come up in this context are highly nontrivial, and several apparently obvious limits have later been proved to be no real limits. As an example, it was believed that, since a logic gate changes a degree of freedom of a physical system, it must therefore dissipate at least the energy kT.

As the Fig. 7 shows, the energy dissipated per logical step has decreases by more than ten orders of magnitude over the last fifty years. Within 10-15 years, this quantity will reach the thermal energy kT. This implies that some schemes for performing calculations will no longer work. It is now established, however, that information can be processed with techniques that dissipate less than kT per logical step. There is no lower limit for the energy required for a logical operation, as long as the time is not critical.

3.1 Information and Thermodynamics

The flow of information corresponds to a transfer of entropy. Information processing is therefore closely tied to thermodynamics. As an introduction to these issues consider the problem the Maxwell demon: As Maxwell discussed, in his *"Theory of heat"* in 1871,

> *"If we conceive a being whose faculties are so sharpened that he can follow every molecule in its course, such a being, whose attributes are still essentially finite as our own, would be able to do what is at present impossible to us. For we have seen that the molecules in a vessel full of air at uniform temperature are moving with velocities by no means uniform..."*

Now let us suppose that such a vessel is divided into two portions, A and B, by a division in which there is a small hole, and that a being, who can see the

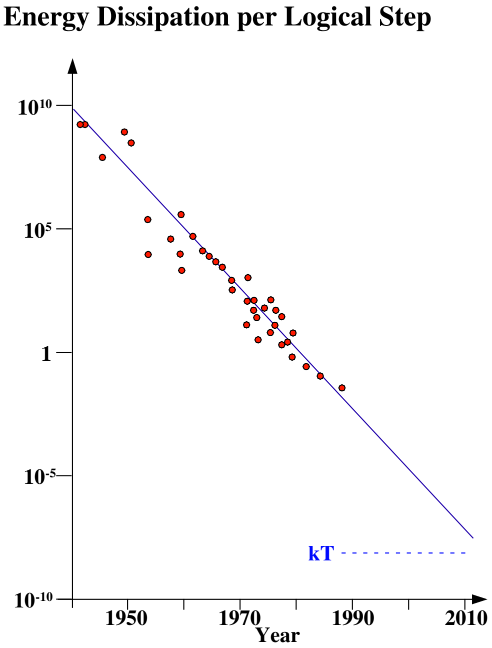


Figure 7: Historical and predicted energy dissipation per logical step.

individual molecules, opens and closes this hole, so as to allow only the swifter molecules to pass from A to B, and only the slower one to pass from B to A. He will thus, without expenditure of work, raise the temperature of B and lower that of A, in contradiction to the second law of thermodynamics." Clearly such a device is not in contradiction with the first law of thermodynamics, but with the second.

Decisions equals information – A number of people discussed this issue, adding even simpler versions of this paradox. A good example is that the demon does not have to measure the speed of the molecules; it is sufficient if he measured its direction: He only opens the door if a molecule comes towards the door from the left (e.g.), but not if it comes from the right. As a result, pressure will increase in the right hand part of the container. This will not create a heat-difference, but rather a pressure difference, which could also be used as a source of energy. Still, this device does not violate conservation of energy, since the energy of the molecules is not changed. The first hint at a resolution of this paradox came in 1929 from Leo Szilard [19], who realized that the measurement, which must be taken on the molecules, does not come for free: the information required for the decision, whether or not to open the gate, compensates the entropy decrease in the gas. It is thus exactly the information processing, which prevents the

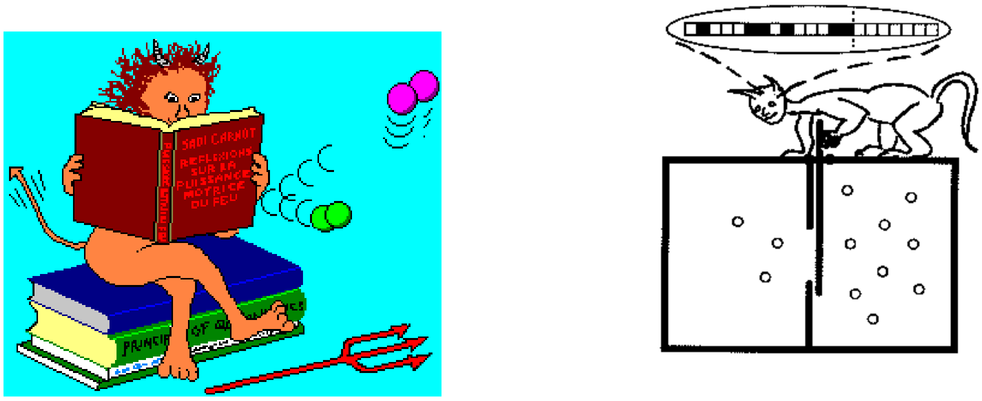
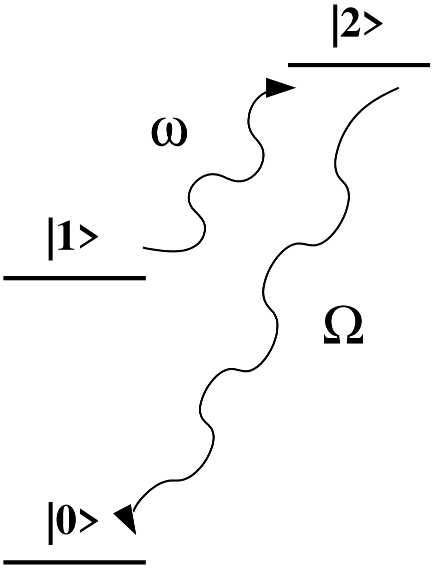
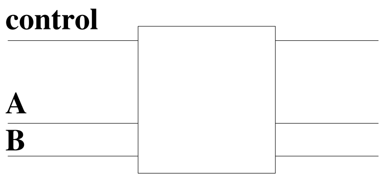


Figure 8: Maxwell's demon. In this illustration the demon sets up a pressure difference by only raising the partition when more gas molecules approach it from the left than from the right. This can be done in a completely reversible manner, as long as the demon's memory stores the random results of its observations of the molecules. The demon's memory thus gets hotter. The irreversible step is not the acquisition of information, but the loss of information if the demon later clears its memory.

violation of the second law. This fact is illustrated in Fig. 8.

Erasing information – While Szilard's analysis of the situation was correct, he only assumed that this had to be the case, he did not give a proof for this assumption. It was Rolf Landauer of IBM [20] who made a more careful analysis, explicitly discussing the generation of entropy in various computational processes. Other researchers, including Charles Bennett, Edward Fredkin, and Tommaso Toffoli showed that it is actually the process of erasing the information gained during the measurement (which is required as a step for initializing the system for the next measurement) creates the entropy, while the measurement itself could be made without entropy creation. Erasing information is closely related to dissipation: a reversible system does not destroy information, as expressed by the second law of thermodynamics. Obviously most current computers dissipate information. As an example consider the calculation $3 + 5 = 8$: It is not possible to reverse this computation, since different inputs produce this output. The process is quite analogous to the removal of a wall between two containers, which are filled with different pressures of the same gas. The creation of entropy during erasure of information is always associated with dissipation of energy. Typically, the erasure of 1 bit of information must dissipate at least an energy of kT. This can be illustrated in a simple picture: We assume that the information is stored in a quantum mechanical two-level system, the two states being labeled $|0>$ and





Input			Output		
control	A	B	control	A	B
1	1	1	1	1	1
1	1	0	1	0	1
1	0	1	1	1	0
1	0	0	1	0	0
0	1	1	0	1	1
0	1	0	0	1	0
0	0	1	0	0	1
0	0	0	0	0	0

Figure 9: Left: Electromagnetic information eraser: Light with frequency ω will do nothing to a state in $|0\rangle$ and promote $|1\rangle$ to a third state $|2\rangle$. Spontaneous emission will bring it then to $|0\rangle$. This process is incoherent since the phases of the photons are not observed. Right: The Fredkin gate, not that every three-tuple (x, y, z) appears exactly once on input and output, it is reversible.

$|1>$. Erasing the information contained in this bit can be achieved by placing it in state $|0>$, e.g., independent of its previous state. This is obviously impossible by unitary operations, i.e. by (energy-conserving) evolution under a Hamiltonian.

Information loss by dissipation – A possible procedure to erase information uses spontaneous emission (which is non-unitary) from a third state $|2>$, which must have an energy higher than that of state $|0>$, see Fig. 9. We use an electromagnetic pulse that is resonant with the transition $|1> -|2>$. If the system is initially in state $|1>$, the pulse puts in in state $|2>$. If it is initially in state $|0>$, the pulse does nothing. From state $|2>$, the system will undergo spontaneous emission By a proper choice of state, it can be arranged that the system is most likely to end up in state $|0>$. If this probability is not high enough, the procedure must be repeated. The minimum energy expenditure for this procedure is defined by the photon energy for bringing the system into the excited state. This energy must be larger than kT, since the system could otherwise spontaneously undergo this transition, driven by the thermal energy. Similar requirements hold in classical systems, where dissipation is typically due to friction.

3.2 Reversible Logic

As discussed in Sec. 2, conventional computers use Boolean logic, which includes the operations AND and OR. Both these operations, which have two input bits and one output bit, discard information, i.e. they reduce the phase space.

Entropy generation – This requires the generation of entropy at some other place. The entropy generated by erasing a bit of information is $\Delta S = kT \ln 2$. Computers based on Boolean logic are therefore inherently dissipative devices. This generation of heat during the computational process represents an obvious limitation, since no physical device can withstand arbitrary amounts of heat generation.

Dissipationless computation – It turns out, however, that computers do not have to rely on Boolean logic. They can use, instead, reversible logic, which preserves the information, generating no entropy during the processing. Examples of reversible computation include quantum mechanical processes, where the computation can be written as a sequence of unitary operations, which are always reversible. For this particular case, it is easy to prove that the energy dissipated during the computation $< E > (t) - < E > (0)$ is zero:

$$
\begin{aligned}
< E > (t) &= \mathrm{Tr}\left(H\rho(t)\right) = \mathrm{Tr}\left(H \exp(-iHt)\rho(0)\exp(iHt)\right) = \\
&= \mathrm{Tr}\left(\exp(iHt) H \exp(-iHt)\,\rho(0)\right) = < E > (0)\ .
\end{aligned}
$$

Reversible computation – A general reversible computer can be represented as a system of states, corresponding to the information stored in the computer, and a sequence of logical operations, transforming one such state into the next. Since no information is discarded, it is possible to reverse to complete computation and bring the system back to its initial state, simply be reversing each of the logical operations. No minimum amount of energy is required to perform reversible logical operations.

The Fredkin gate – The first proof that reversible logic gates can form the basis of a universal computer is due to Fredkin. He proposed a three-bit gate that is now known as the Fredkin gate:

$$
(x, y, z) \longrightarrow (x, xy + (1-x)z, xz + (1-x)y)\ .
$$

The three lines (x, y, z) are labeled as control, A and B. If the control bit is 1, the Fredkin gate interchanges A with B, otherwise it leaves them untouched. The Fredkin gate is reversible, as can be seen from the truth table in Fig. 9. The Fredkin gate can be used to implement a reversible AND gate by identifying the inputs of the AND gate with the control and A input of the Fredkin gate and setting the B input line of the Fredkin gate to 0.

$$
(x, y, 0) \longrightarrow (x, xy, (1-x)y) \equiv (x, x \text{ AND } y, (1-x)y)\ .
$$

The output A then contains the output of the AND gate, while the control and B lines contain bits of information which are not used by the boolean logic, but would be required to reverse the computation. We can use the Fredkin gate, as well as the Toffoli gate discussed in Sec. 2.2.2, in order build a classical reversible computer.

The reversible Turing machine – Another reversible computational architecture is a reversible Turing machine. A Turing machine consists of an infinitely long tape storing bits of information, a read/write head that can be in a number of different states, and a set of rules what the machine is to do depending on the value of the bit at the current position of the head and the state of the head. A (possible) reversible set of rules would be

head state	bit read	change bit to	change state to	move to
A	1	0	A	left
A	0	1	B	right
B	1	1	A	left
B	0	0	B	right

Lecerf [10] and independently Bennett [41] showed that an irreversible Turing machine can be simulated with a reversible Turing machine, at the expense of extra computer space and time. This is a remarkable fact for quantum computing since a quantum Turing machine must be reversible.

3.3 The ultimate Laptop

Some limits to the performance of computers have been summarised by Seth Lloyd [21] in a very popular style: he discusses the "ultimate laptop", i.e. the maximum performance that a computer of 1 kg mass and 1 l of volume may ultimately achieve.

Uncertainty principle – One limit can be derived from the uncertainty principle: It can be shown [22] that it takes at least a time

$$\Delta t \;=\; \frac{\pi\hbar}{2E} \tag{3}$$

for a quantum mechanical state to evolve into an orthogonal state, if E is the energy of the system. This relation is physically pretty obvious, since time and energy are canonical conjugate variables in quantum mechanics.

Two-level system – Let us consider a two-level system $|\alpha\rangle$ and $|\beta\rangle$. We set the energy of the ground state $|\alpha>$ to zero, the excited state $|\beta>$ has then an energy $\hbar\omega_L$. An initial state

$$\Psi(0) \;=\; \frac{1}{2}\Big(|\alpha\rangle + |\beta\rangle\Big)$$

then evolves under time evolution into

$$\Psi(t) \;=\; \frac{1}{2}\Big(|\alpha\rangle + e^{-i\omega_L t}|\beta\rangle\Big)$$

Apparently the two states are orthogonal for $\omega_L t = \pi$, i.e. after $t = \pi/\omega_L$. Since the (constant) energy of this state is $E = \hbar\omega_L/2$, we recover the condition (3).

General consequences – An interesting aspect of the limit (3) is that it does not depend on the architecture of the computer. While we generally expect computers containing many processors working in parallel to be faster than purely serial computers, this is no longer the case for a computer working at the limit just discussed: if the number of processors increases, the available energy per processor decreases and correspondingly its speed. The total number of logical operations per unit time remains constant.

Limits by the number of atoms – The finite number of atoms in a computer can be considered a limit to computation. For a mass of 1 kg, this would be of the order of 10^{25}. In NMR and ion trap quantum computers, each atom stores one bit of information. At this density, it would thus be possible to store 10^{25} qubits of information in a computer. If optical transitions of these atoms are used for logical operations, gate times of the order of 10^{-15}s would be feasible, allowing a total of 10^{40} logical operations per second for the whole computer. At such data rates, the different parts of the computer would not be able to communicate with each other at the same rate as the individual logical operations. The computer would therefore need a highly parallel architecture. †

Deviations from Moore's law – While this limit of 10^{40} logical operations per second appears very remote, it would only take of the order of 100-200 years of progress at the current rate (as summarized by Moore's law) to actually reach this and related limits. It is therefore very likely that a deviation from Moore's law will be observed within this time frame.

Entropy in data storage – A limit on the amount of data stored in the computer can be derived from thermodynamics. According to statistical mechanics, the entropy of a system is

$$S \;=\; k_B \ln W,$$

where W is the number of accessible states. To store N bits of information, we need N two-level systems, which have 2^N states. Accordingly, a system that stores N bits has an entropy

$$S = N k_B \ln 2,$$

†If serial operation is preferred (which may be dictated by the algorithm), the computer needs to be compressed. Fully serial operation becomes possible only when the dimensions become equal to the Schwarzschild radius ($= 1.485 \times 10^{-27}m$ for $m = 1kg$), i.e. when the computer forms a miniature black hole.

It should be realized here, that the entropy that we calculate is the entropy of an ensemble at a given energy, while the actual system doing the computation is in a well-defined (pure) state, thus having zero entropy.

Error corrections – Detecting an error can in principle be achieved without energy dissipation. However, correcting it implies eliminating information (to the environment), thus generating dissipation. The entropy per bit comes therefore in play for error corrections. Let's assume we want to be able to correct $\dot{N}$ errors per second, i.e. we have an entropy production of $\dot{S} = \dot{N} k_B \ln 2$ per second. This corresponds via

$$\frac{\delta Q}{T} \;=\; \Delta S$$

to a heat production of

$$\dot{Q} \;=\; \dot{N}(k_B T)\ln 2$$

per second. If we assume that this heat is transported out of the system by heat conduction we have

$$\dot{N}(k_B T)\ln 2 \;=\; \dot{Q} \;=\; \kappa\, A\, \frac{\Delta T}{\Delta x}\ ,$$

where κ is the thermal conductivity, ΔT the Temperature difference in between the computer and the cooling environment, A the area used for cooling and Δx the distance over which the heat is transported. Let's assume $A = 1\,\mathrm{m}^2$, $\Delta T = 100\,\mathrm{K} = T$ $\Delta x = 1\,\mathring{A} = 10^{-10}\mathrm{m}$. Typical (good) thermal conductivities are of the order of $100\,\mathrm{W/(mK)}$. We then obtain a limit of (only) $10^{12}/\ln 2$ error corrections per second.

References

[1] Michael Brooks. *Quantum Computing and Communications*. Springer, New York, 1999. 152 pp.

[2] Jozef Gruska. *Quantum computing*. McGraw-Hill, London, 2000. 439 pp.

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge Univ. Press, Cambridge, 2001. 676 pp.

[4] Colin P. Williams and Scott H. Clearwater. *Explorations in quantum computing*. Springer, New York, 1998. 307 pp, CD-ROM, DM 98.00.

[5] A. Steane. Quantum computing. *Rep. Prog. Phys.*, 61:117–173, 1998.

[6] Dorit Aharonov. Quantum computation. In Dietrich Stauffer, editor, *Annual Reviews of Computational Physics VI*, pages 259–346. World Scientific, 1999. Preprint quant-ph/9812037.

[7] A. Galindo and M. A. Martin-Delgado. Information and computation: Classical and quantum aspects, 2002. Rev. Mod. Phys., to appear. Preprint quant-ph/0112105.

[8] John Preskill. Quantum computation. http://theory.caltech.edu/ preskill/ph229/, 1997. 413 pp.

[9] Paul Benioff. Quantum mechanical Hamiltonian models of Turing machines. *J. Stat. Phys.*, 29:515, 1982.

[10] Y. Lecerf. Machines de Turing reversibles. Compters Rendus **257**, 1597, 1963.

[11] Richard P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467–488, 1982.

[12] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. In *Proceedings, 35th Annual Symposium on Foundations of Computer Science*, Piscataway, NJ, 1994. IEEE Press.

[13] Stephan Mertens. Computational complexity for physicists. Lecture given at the DPG school on "Quantum Computing", 2000. Preprint cond-mat/0012185.

[14] Barenco, A., C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter. *"Elementary gates for quantum computation"*, Phys. Rev. A **52**, 3457-3467 (1995).

[15] Barenco, A., D. Deutsch, A. Ekert and R. Jozsa. *"Conditional quantum dynamics and logic gates"*, Phys. Rev. Lett. **74**, 4083-6 (1995).

[16] Alonzo Church. An unsolvable problem of elementary number theory. *Am. J. Math.*, 58:345–363, 1936.

[17] Alan M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc. Ser.*, 42:230, 1936. See also ibidem 43, 544.

[18] Douglas R. Hofstadter. *Gdel, Escher, Bach: An Eternal Golden Braid*. Basic Books, New York, 1979. 777 pp.

[19] Leo Szilard. ber die Entropieverminderung in einem thermodynamischen System bei Eingriffen intelligenter Wesen. *Z. Physik*, 53:840–856, 1929.

[20] R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal Res Dev*, 5:183–191, 1961.

[21] Seth Lloyd. Ultimate physical limits to computation. *Nature*, 406:1047–1054, 2000.

[22] N. Margolus and L.B. Levitin. title. In T. Toffoli, M. Biafore, and J. Le?o, editors, *Proceedings of the Fourth Workshop on Physics and Computation PhysComp96 (New England Complex Systems Institute, Boston, MA, 1996)*. North-Holland, 1998. Physica D Vol. 120.

[23] Richard P. Feynman. *Feynman Lectures on Computing*, chapter 6, Quantum Mechanical Computers. Addison-Wesley, 1996. Originally published in Optics News, February 1985, pp. 11-20; see also Found. Phys. **16**, 507-532 (1986).

[24] P. Jordan and E. Wigner. Über das Paulische Äquivalenzverbot. *Z. Physik*, 47:631–651, 1928.

[25] Jian-Wei Pan, Dik Bouwmeester, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger. Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement. *Nature*, 403:515–519, 2000.

[26] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe. Experimental entanglement of four particles. *Nature*, 404:256–259, 2001.

[27] Rainer Blatt. Push-button entanglement. *Nature*, 404:231–232, 2001.

[28] Brian Julsgaard, Alexander Kozhekin, and Eugene S. Polzik. Experimental long-lived entanglement of two macroscopic objects. *Nature*, 413:400–403, 2001.

[29] J. Ignacio Cirac. Quantum physics: Entangled atomic samples. *Nature*, 413:375–377, 2001.

[30] L. Grover. (title). In *Proc. 28th Annual ACM Symposium on the Theory of Computation*, pages 212–219, New York, 1996. ACM Press.

[31] L.K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, 1997. Preprint quant-ph/9706033.

[32] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing, 1999. Preprint quant-ph/9906054.

[33] D.P. DiVincenzo. The physical implementation of quantum computation. *Fortschr. Phys.*, 48:771–783, 2000. Preprint quant-ph/0002077.

[34] C.E. Hughes and S. Wimperis. Bounds on spin dynamics and the design of multiple-pulse NMR experiments. *J. Chem. Phys.*, 106:2105–2117, 1997.

[35] J. Stoustrup, O. Schedletzky, S.J. Glaser, C. Griesinger, N.C. Nielsen, and O.W. Sorensen. Generalized bound on quantum dynamics: efficiency of unitary transformations between non-hermitian states. *Phys. Rev. Lett.*, 74:2921–2924, 1995.

[36] J. H. Smet, R. A. Deutschmann, F. Ertl, W. Wegscheider, G. Abstreiter, and K. von Klitzing. Gate-voltage control of spin interactions between electrons and nuclei in a semiconductor. *Nature*, 415:281–286, 2002.

[37] J. Kikkawa. Eavesdropping on spin talk. *Nature*, 415:273–274, 2002.

[38] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[39] D. Dieks. Communication by EPR devices. *Phys. Lett. A*, 92:271–271, 1982.

[40] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[41] C.H. Bennettr. Logical reversability of computation. *IBM J. Res. Dev.* **17**, 525-532, 1973.

[42] C.H. Bennett and S.J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, 1992.

[43] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India, December 1984)*, pages 175–179, New York, 1984. IEEE.

[44] H. Zbinden, J.D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittle. Interferometry with Faraday mirrors and quantum cryptography. *Electron. Lett.*, 33:586–588, 1997.

[45] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

[46] G.M. Palma, K.-A. Suominen, and A.K. Ekert. Quantum computers and dissipation. *Proc. Roy. Soc. A*, 452:567–584, 1996.

[47] D.A. Lidar, I.L. Chuang, and K.B. Whaley. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.*, 81:2594–2597, 1998.

[48] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84:2525–2528, 2000.

[49] L. Viola, E.M. Fortunato, M.A. Pravia, E. Knill, R. Laflamme, and D.G. Cory. Experimental realization of noiseless subsystems for quantum information processing. *Science*, 293:2059–2063, 2001.