Spin qubits in solid-state structures

Guido Burkard and Daniel Loss
Department of Physics and Astronomy, University of Basel, Klingelbergstrasse 82, CH-4056 Basel, Switzerland

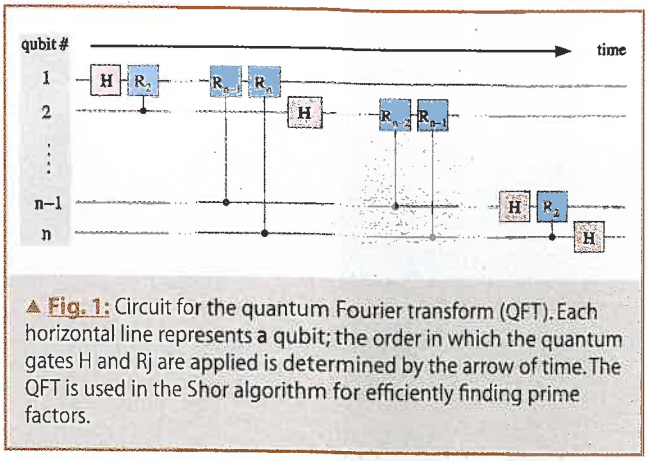
It is remarkable that today's computers, after the tremendous development during the last 50 years, are still essentially described by the mathematical model formulated by Alan Turing in the 1930's. Turing's model describes computers which operate according to the laws of classical physics. What would happen if a computer was operating according to the quantum laws? Physicists and computer scientists have been interested in this question since the early 1980's, but research in quantum computation really started to flourish after 1994 when Peter Shor discovered a quantum algorithm to find prime factors of large integers efficiently, a problem which is intrinsically hard for any classical computer (see [1] for an introduction into quantum computation). The lack of an algorithm for efficient factoring on a classical machine is actually the basis of the widely used RSA encryption scheme. Phase coherence needs to be maintained for a sufficiently long time in the memory of a quantum computer. This may sound like a harmless requirement, but in fact it is the main reason why the physical implementation of quantum computation is so difficult. Usually, a quantum memory is thought of as a set of two-level systems, named quantum bits, or qubits for short. In analogy to the classical bit, two orthogonal computational basis states $|0\rangle$ and $|1\rangle$ are defined. The textbook example of a quantum two-level system is the spin 1/2 of, say, an electron, where one can identify the "spin up" state with $|0\rangle$ and the "spin down" state with $|1\rangle$. While several other two-level systems have been proposed for quantum computing, we will devote the majority of our discussion to the potential use of electron spins in nanostructures (such as quantum dots) as qubits.

Shor's factoring algorithm

We return to Shor's algorithm, since it allows us to explain many important concepts. At the heart of it lies the quantum Fourier transform (QFT). Given n qubits with an orthonormal basis $|0\rangle,\ldots,|2^n-1\rangle$, the QFT is a unitary $2^n\times 2^n$ matrix $U_{\rm QFT}$ such that

$$U_{\rm QFT}|j\rangle = 2^{-n/2}\sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n}|k\rangle. \qquad (1)$$

The QFT can be decomposed into a series of elementary operations, as shown in Fig. 1. The elementary operations, or "gates", used here can be described as follows. The Hadamard gate H acts on a single qubit (represented by a horizontal line in Fig. 1). It transforms $|0\rangle$ into $(|0\rangle+|1\rangle)/\sqrt{2}$ and $|1\rangle$ into $(|0\rangle-|1\rangle)/\sqrt{2}$. The gate R_j denotes a rotation of the qubit by an angle of $2\pi/2^j$ about the z axis. The vertical line which connects the box with R_j to another qubit means that this is a controlled rotation, i.e. the target qubit (below the box) is rotated if the control qubit (marked with the dot) is in state $|1\rangle$ and left unchanged otherwise. This description defines the controlled-R_j gate uniquely for all initial states of the control and target qubits since it determines its operation on a basis of products of $|0\rangle$ and $|1\rangle$.



▲ **Fig. 1:** Circuit for the quantum Fourier transform (QFT). Each horizontal line represents a qubit; the order in which the quantum gates H and Rj are applied is determined by the arrow of time. The QFT is used in the Shor algorithm for efficiently finding prime factors.

The controlled-R_j is an example for a two-qubit quantum gate. Quantum gates acting on more than one qubit are necessary in order to perform non-trivial quantum logic. Fortunately, it is possible to make use of only one two-qubit gate (e.g., the controlled-NOT) in combination with single-qubit gates for doing any quantum computation. Controlled-NOT (also called XOR) is similar to controlled-R_j, but with the qubit rotation replaced by an inversion $|0\rangle\leftrightarrow|1\rangle$.

The number of elementary quantum gates in the QFT circuit shown in Fig. 1 grows as the square of the number $n=\log_2 N$ of qubits which are required to store the input N, whereas the classical fast Fourier transform (FFT) takes roughly $n2^n$ steps. It was Shor's idea to apply period finding with the QFT to factor a number $N=0,\ldots,2^n-1$: the period of the function $f(x)=a^x \bmod N$ can be used to find a prime number not equal to 1 or N which divides N. Here, a is a random number between 1 and $N-1$ which has no common divisor with N (if it has, the problem is solved). Everything taken together, the number of elementary operations needed for finding a prime factor of N with the Shor algorithm essentially scales with n^2, while the most efficient classical algorithm known presently requires exponentially more, on the order of $\exp(n^{1/3}\log^{2/3}n)$. In order to illustrate the difference between power law (quantum) and exponential (classical) scaling, let us assume for the moment that we had both a classical computer and a quantum computer running Shor's algorithm, and that both of them required one hour for factoring a number with 100 decimals. To find a prime factor of a number with 1000 decimals would then take about a week on the quantum computer while using the classical computer, it would require about 10^{12} years, longer than the estimated age of the universe!

Beyond Factoring

Besides finding prime factors, the QFT can be used to solve other problems efficiently for which there is no efficient classical method. Consider for example the problem of discrete logarithms (which, as the factoring problem, has applications in cryptography): given integers a and $b=a^s$, find the value of the integer s. There is a whole class of problems of this kind which relate in some way to the problem of finding the period of a discrete function.

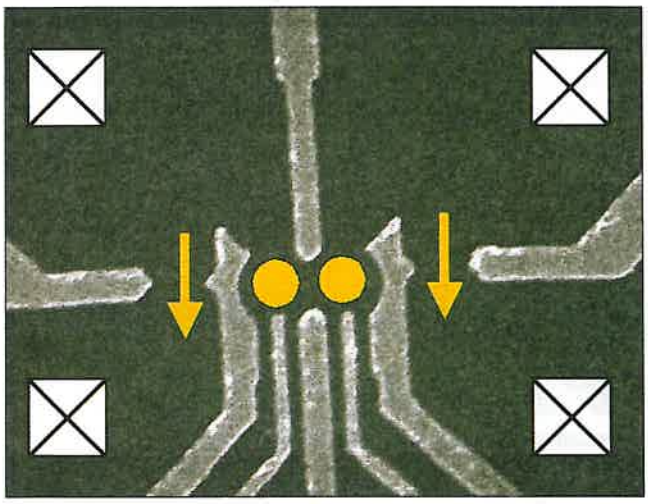
Another class is represented by Grover's algorithm which finds an element in an unsorted database containing N entries. Solving this problem is like knowing a phone number and looking up the corresponding name in a phone book having N entries. Grover's algorithm requires $\propto\sqrt{N}$ elementary gate operations, while the fastest classical method requires $\propto N$ steps.

One of the early ideas is to use a controlled quantum system (quantum computer) to simulate another quantum system. When quantum systems are simulated on classical computers the computation time generically scales exponentially with the size of the system. Given a local Hamiltonian defined on a discrete (or discretized) system and some initial state, there is a quantum algorithm that computes the final state up to an accuracy ε with a number of elementary quantum gates which scales as a power of $1/\varepsilon$.

State of the Art

Recently, Shor's algorithm was implemented using nuclear magnetic resonance (NMR) with an ensemble of molecules in solution containing $n = 7$ nuclei with spin-1/2 addressed individually with rf fields [2]. This machine was able to factor the number 15. Nobody was particularly surprised that the answer was $15 = 3 \cdot 5$, but the experiment is still remarkable and represents the current state of the art of quantum computation. The regime where quantum computers could "boldly go where no classical computer has gone before" (and, e.g., break RSA encryption keys) starts at around $n = 1000$ qubits and millions of elementary quantum gates. It is fair to say that nobody knows whether there will ever be a quantum computer which will accomplish this. On the other hand, it is quite certain that room-temperature liquid NMR will never reach this stage. The most important reason for this is that only ensemble averages are experimentally accessible and at the temperatures available these average signals decrease exponentially as the number of qubits increases. It also is not obvious how to make molecules or similar structures with, say, a thousand spins which can be individually addressed. Moreover, there have been theoretical arguments whether NMR quantum computing is really "quantum" (see [3] and references therein).

There are other systems, in which elementary quantum operations have already been performed experimentally [3], the most prominent examples being ion traps and high-Q optical cavities. Although, in contrast to NMR, these two implementations allow the manipulation and read-out of individual qubits, it appears rather difficult to scale them up to a large number of qubits.



▲ **Fig. 2:** Scanning electron micrograph of a semiconductor structure with two coupled quantum dots (yellow disks) formed by applying a negative bias to the metallic contacts (grey) which define the quantum dots. The electron number in each dot can be controlled down to one, and it can be measured by quantum point contacts (yellow arrows). [courtesy of L. Kouwenhoven, TU Delft]

Electron Spins as Qubits

Motivated by the rapid upscaling of microelectronic semiconductor devices, several solid-state implementations of quantum computing have been proposed. The analogy with the development of classical circuits even led some researchers to call the ion trap a "vacuum tube quantum computer" (the fate of the vacuum tube was to be superseded by a solid state device-the transistor). Here, we concentrate on the idea put forward in early 1997 by Loss and DiVincenzo to use the spin 1/2 of electrons in confined nanostructures, e.g. quantum dots, as qubits (see chapter 8 in [4] for a review). Many solid-state implementations for quantum computing have been proposed subsequently [3], including superconducting qubits, nuclear spins of donor atoms in silicon, and charge qubits in quantum dots.

The electron's spin is a "natural" representation of a qubit since it comprises exactly two levels. Unlike for charge states in an atom or quantum dot, there are no additional degrees of freedom into which the system could "leak". Another great advantage of spins as compared to charge qubits is that in typical semiconductor materials like gallium arsenide (GaAs) or silicon (Si), the time over which the spin of a conduction-band electron remains phase coherent can be several orders of magnitude longer than the corresponding charge decoherence times. Of course these numbers have to be compared with the time it takes to perform an elementary gate operation. Even considering this, single spins seem to be very well suited as qubits. The transverse decoherence time T_2, which is most relevant in the context of quantum computing, is defined as the characteristic time over which a single spin which is initially prepared as a coherent superposition of "spin up" and "spin down" coherently precesses about an external magnetic field. The transverse dephasing time $T_2^* \leq T_2$ of an ensemble of spins in n-doped GaAs can exceed 100 ns, as demonstrated by optical measurements [5], while switching times are estimated to be on the order of 10–100 ps. The longitudinal (energy) relaxation time T_1 determines how long it takes for a non-equilibrium spin configuration to relax to equilibrium. T_1 can be much longer than T_2 (and particularly long in confined structures), but while suppression of spin relaxation is necessary for quantum computation, it is not sufficient.

In the battle against decoherence, physics is also helped by the results of fundamental research in quantum information theory. Error correcting codes have been developed which in principle allow arbitrary long quantum computations to be performed even in the presence of decoherence and imperfect quantum gates, as long as the error rate does not exceed a certain threshold. This threshold depends on the error model and the code; typical numbers are around 1 memory or gate error in 10^4 cycles.

Quantum Dots

Semiconductor quantum dots are small islands of electrons in an otherwise depleted region. The largest degree of control can be obtained with quantum dots that are electrically confined in a two-dimensional electron system (2DES) formed e.g. at the interface between a GaAs and an AlGaAs layer or in a quantum well formed by an AlGaAs-GaAs-AlGaAs "sandwich". Using metallic gates at the top of the heterostructure, electrons can be laterally confined to a region with a size on the order of the Fermi wavelength (around 40 nm in a typical GaAs/AlGaAs 2DES), leading to a discrete energy spectrum (quite like in atoms). A quantum dot can be connected to external leads via tunneling

contacts which are likewise formed in the 2DES by electrical gating. In these systems, the Coulomb blockade effect, i.e. the quantization of the electronic charge on the dot which leads to pronounced peaks in the conductance as a function of an applied gate voltage, can be observed.

Adjacent quantum dots can be coupled, as shown in Fig. 2. In the Coulomb blockade regime, adding and removing single electrons is easy, however, removing all but one electron is very hard and has been achieved only recently in lateral dots like those in Fig. 2.

In order to use electron spins for quantum computation, one would like to label them in order to be able to address a certain qubit at any time during the computation and for the read-out of the final result. If the electrons carrying the spin qubits were free like in a metal or 2DES, then this would be impossible due to the indistinguishability of identical particles in quantum mechanics. However, if the electrons carrying the quantum information were localized in an array of quantum dots (Fig. 3) then they could be distinguished by their position.

Exchange Coupling

As mentioned earlier, for quantum computing qubits need to be coupled using a two-qubit gate. In the case of localized spins the required coupling can be obtained via tunneling between adjacent dots. This can be understood in terms of a simple Hubbard model with a tunneling amplitude t between adjacent sites and an on-site Coulomb repulsion energy U. With one electron per dot, one finds in the limit $t \ll U$ that the low-energy physics of the system is described by the spin Hamiltonian

$$H = \sum_{1\le i<j\le n} J_{ij}\mathbf{S}_i \cdot \mathbf{S}_j + \mu_B \sum_{1\le i\le n} g_i \mathbf{B}_i \cdot \mathbf{S}_i, \qquad (2)$$

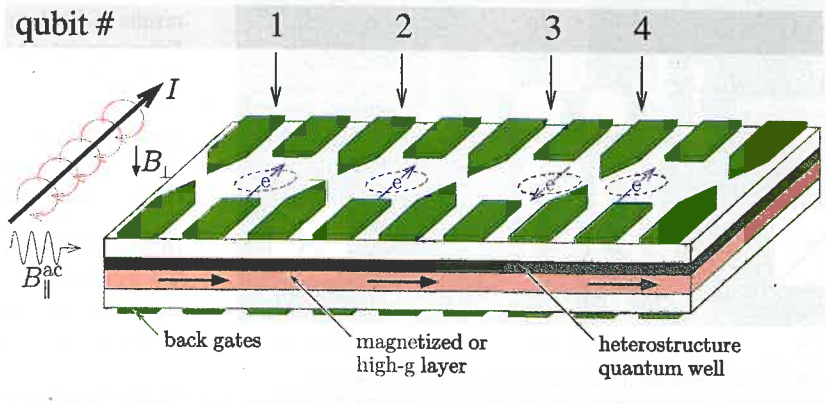
where $\approx = 4t^2/U$ is the exchange energy and $\mathbf{S}_i$ denotes the spin 1/2 operator at site i. We have also included the Zeeman energy due to an external magnetic field $\mathbf{B}_i$ at site i, where μ_B is the Bohr magneton and g_i is the Landé g-factor. Even if the external field is constant and homogeneous, both the exchange for each pair of spins and the Zeeman term for each individual spin (see below) can be controlled by electrical gating. Applying a gate voltage at the surface will increase the potential barrier for electrons between adjacent dots, and J will be reduced exponentially. This effectively provides a mechanism for switching on and off the coupling between two qubits while all other interactions are off (this is required for a circuit as e.g. Fig. 1). In NMR however, all interactions are on all the time, and one has to apply refocusing techniques in order to "effectively" switch off the unwanted interactions.

One can use the analogy between quantum dots and atoms and treat the coupled system as an artificial hydrogen molecule. Since the exchange energy is just the energy difference between the lowest spin singlet and triplet states of a two-electron system, we can find a good estimate for J by applying the Heitler-London method from molecular physics. For more details and for a number of improvements to the Heitler-London method we refer the interested reader to chapter 8 in [4]. Molecular states in quantum dots have been observed in the Coulomb blockade regime, but further evidence is required to distinguish between single-electron states ("H_2^+ molecules") and the two-electron states discussed here ("H_2 molecules").

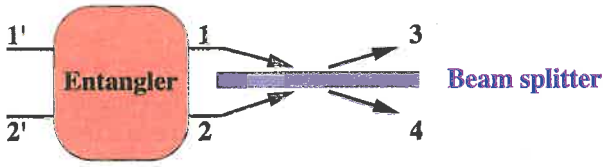
Quantum dot quantum logic

If the exchange coupling between two neighboring spins is switched on for a finite amount of time and the time-integrated exchange energy (divided by $\hbar$) equals exactly π then the states of the two spins are swapped. For quantum computation, the "square-root of swap" ($\sqrt{SWAP}$), obtained by applying a time-integrated exchange of only $\pi/2$, is much more interesting: it can be used to produce a maximally entangled state of two spins from a product state. An example is the spin singlet state $|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle$. Entanglement is one of the essential features of quantum mechanics and thus plays a key role in quantum computing (the connection between entanglement and the efficiency of quantum algorithms is still not fully understood). $\sqrt{SWAP}$ can be combined with single-qubit gates into the controlled-NOT gate. As a consequence, the exchange interaction between spins plus the ability to rotate single spins is sufficient for quantum computation.

During the short time of the switching process (not in between), the spin of the electrons in the coupled quantum dots is coupled to the charge via the Pauli exclusion principle, and we have to avoid charge excitations. The relevant energy scales are the



▶ **Fig. 3:** Sketch of a linear array of quantum dots (dashed circles), each containing a single (excess) spin 1/2 (blue arrow) representing a qubit for quantum computing. Localized spins can be labeled and addressed individually. The metal gate electrodes (green) are used to define the quantum dots and the couplings between them. For single-qubit operations, a local difference in Zeeman splittings could be achieved electrically, e.g. by applying a gate potential between the top and the bottom of the structure; any electron can then be shifted individually towards a magnetized or high-g layer (red). Likewise, such local Zeeman splittings could be generated by a static inhomogeneous magnetic field, e.g. produced by a current I (red circles). Single-qubit rotations could be performed using electron spin resonance (ESR) with a homogeneous oscillatory field $B_\parallel^{ac}$ with a frequency matching the local Zeeman splitting of the desired qubit. The exchange coupling between adjacent spins could also be controlled electrically by gate electrodes. We have sketched a situation where the qubits 3 and 4 are coupled.



▲ Fig. 4: Setup for detecting entangled electrons which are injected from the entangler into Fermi leads 1 and 2. Two-particle interference at the electronic beam splitter leads to distinct statistical effects for entangled singlet or triplet pairs in the noise correlations between the outgoing leads. In the case of the singlet, the noise enhancement allows to uniquely detect the entangled state.

level spacing δE on a single quantum dot and the on-site Coulomb repulsion energy U. Typically, both of these energies are several tens of Kelvin, while for smaller quantum dots, they can even approach room temperature. The operating temperature of the quantum computer should not exceed these energies. Furthermore, the switching of external parameters leading to a time-dependent exchange $J(t)$ should not be too fast. One can find optimal switching pulse shapes (e.g. 1/cosh) and lower bounds for the switching times (for typical lateral dots around 100 ps) [4].

Rotating spins

Rotating single spins may seem easier than coupling two spins. However, one finds that applying a field of, say, 1 Tesla to a particular spin without rotating neighbors at a distance of only about 50 nm would require huge field gradients. Although some technologies allow to apply strongly localized magnetic fields (hard disk read/write heads, magnetic force microscope tips), it appears very difficult to achieve large gradients. It seems more realistic to apply electric gate voltages locally, as shown in Fig. 3, changing the vertical position of the localized electrons, which, in combination with a spatially varying Zeeman effect (using either magnetic or g-factor modulated materials), can change the effective magnetic field in which a spin is precessing. This is in principle sufficient for performing arbitrary single-spin rotations-completing the required set of operations for our quantum computer. Modulation of the g-factor by electrical gating was in fact recently demonstrated experimentally at UC Santa Barbara (see [4], chapter 5).

Alternatively, individual spins could be rotated using a homogeneous oscillatory magnetic (ESR) field in combination with a static gradient which allows to select a certain spin by its distinct resonance frequency. Yet another interesting possibility for fast spin manipulation was investigated in Awschalom's group (UCSB). Spin-polarized electrons were rotated using a femtosecond optical pulse which acts like an effective strong magnetic field via the optical Stark effect ([4], chapter 5).

A "computer science" trick to perform universal quantum computation using solely the exchange interaction $JS_i \cdot S_j$ is based on encoding each logical qubit into three spins instead of one. In addition to this overhead the "exchange only" implementation would require on the order of ten times more operations.

Input and Output

A quantum computer would be useless if it were impossible to prepare it initially with some input data and finally to read out the result. Using single-qubit rotations, initializing the system can be reduced to preparation in some fixed known state, such as $|00\ldots0\rangle$. The latter can be produced by applying a homogeneous magnetic field and letting the system relax.

Reading out single spins directly is difficult. As for single-spin rotations, it might be easier to transform the "magnetic" problem into an "electric" one (spin-to-charge conversion). For readout, spin-dependent tunneling to an adjacent empty quantum dot would be monitored using an electrometer (sensitivity orders of magnitude smaller than a single electron charge). The presence or absence of an electron in the adjacent dot after a finite amount of time would then allow one to tell whether there was a spin up or spin down electron in the read dot.

Quantum Communication

It is hard to predict at the moment to what degree and up to which scale quantum computation can ever be realized. Another related field of research, quantum communication, is about to yield new implementable technologies. The most advanced application appears to be quantum key distribution (QKD). The cryptographic keys used nowadays are not unconditionally secure, i.e. they rely on some assumptions which are believed to be true with high confidence, e.g. the widely used RSA scheme for encryption is safe as long as factoring large integers cannot be performed efficiently. The BB84 protocol for QKD, invented by Bennett and Brassard in 1984, is based on the transmission of single qubits (e.g. the polarization of photons) from one party to the other, while a protocol put forward by Ekert in 1991 is based on each of the two parties possessing one qubit of an entangled (or EPR) pair. Quantum teleportation and superdense coding are also based on the use of such entangled pairs. Roughly speaking, two qubits are in an entangled state if their total quantum state cannot be written as the product of quantum states of each qubit separately. So, while $|0\rangle_1 |1\rangle_2$ and $|0\rangle_1 |0\rangle_2 - |0\rangle_1 |1\rangle_2 - |1\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2$ are not entangled, the singlet state $|0\rangle_1 |1\rangle_2 - |1\rangle_1 |0\rangle_2$ is entangled.

All of the concepts mentioned above have been successfully tested using entangled photons from parametric downconversion [1]. There have been several theoretical suggestions to produce, transport, and detect spin entangled electrons in mesoscopic wires [4, 6] and there is increasing experimental effort towards realizing this challenging idea. Actually, entangled states are rather the rule than the exception in condensed matter physics. Particularly interesting are systems which possess entangled ground states (a simple example being two tunnel-coupled quantum dots), since in such a state the entanglement is robust against external perturbations once the system is cooled to low enough temperatures.

The big problem is to harness such entangled states. Using adiabatic pumping, such states could be injected into electrical leads which are attached to quantum dots. Another possible implementation of an "entangler" is a tunnel contact between a conventional BCS superconductor and a normal metal. The ground state of the superconductor consists of a condensate of Cooper pairs which are in the spin singlet. By biasing the superconductor-normal junction, Cooper pairs can be broken and the two resulting electrons can tunnel into the normal metal. In order to be useful for quantum communication, the two electrons have to be extracted in two separate leads while remaining entangled. It has been shown (chapter 8 in [4]) that the fraction of the electrons emerging in separate leads can be drastically increased by connecting the superconductor to two normal quantum dots which are connected to the normal leads such that the on-site Coulomb repulsion in each quantum dot prevents two electrons from simultaneously moving into the same lead.

How can an spin entangler for electrons be tested for its functionality? A solution is to use statistical properties. Due to the Fermi statistics, an electronic spin singlet state has a symmetric orbital wavefunction, and it can be expected that it exhibits "particle bunching" familiar for Bosons in suitable two-particle interference (Hanbury Brown-Twiss) experiments. Consider injecting the electrons from the entangler into an electronic beam splitter (Fig. 4) and then measuring the current autocorrelations in one of the outgoing arms (3 or 4). It can be proven [4, 6] that when the electrons injected are in the entangled spin singlet state, a particle bunching effect will be seen, i.e. the probability for both electrons to emerge in the same (different) outgoing lead will be enhanced (suppressed). This leads to a measurable enhancement of the noise-to-current ratio by a factor of two. Another important issue is whether the spin entanglement becomes degraded owing to electron-electron interactions during transport in the mesoscopic leads. The probability of recovering an entangled pair transmitted through an interacting electron system scales with z_F^4 where $0 < z_F \leq 1$ is the quasiparticle weight. This quantity can be evaluated for a two-dimensional electron system using Green's functions. For typical GaAs samples, $z_F \approx 0.7$, so about 25% of the pairs can be recovered. For weak spin-flip scattering (as seen experimentally e.g. in GaAs), the entanglement of those pairs which are recollected after transmission is still maximal.

Because photons typically interact with their surroundings much more weakly than electrons, they are ideal for long-distance transmission of quantum information, but it is rather hard to couple them to spin-based quantum computer hardware. Besides being of fundamental interest, electron spins, transported over micrometer distances in a solid, serve as a "bus" for the spin-based quantum computer. On the theoretical side, the Fermi statistics for electrons has led to a further generalization of the notion of entanglement.

Outlook

New concepts of quantum information processing are being investigated on the "small scale" with NMR, quantum optics, and trapped ions. Theoretical work on solid-state quantum computing, in particular the spin-based scheme outlined here, has motivated considerable experimental efforts towards solid-state qubits. Regardless of whether a large-scale solid-state quantum computer will emerge from these efforts, it is already now exciting to follow these developments since new and interesting results in both fundamental and applied physics can be expected.

References

[1] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[2] L. M. K. Vandersypen *et al.*, Nature **414**, 883 (2001).

[3] Fortschritte der Physik **48**, Special issue on *Experimental Proposals for Quantum Computation*, eds. H.-K. Lo and S. Braunstein (Wiley-VCH, Berlin, 2000).

[4] *Semiconductor Spintronics and Quantum Computation*, eds. D.D. Awschalom, D. Loss, and N. Samarth, (Springer, Berlin, 2002).

[5] J. M. Kikkawa and D. D. Awschalom, Phys. Rev. Lett. **80**, 4313 (1998).

[6] G. Burkard, D. Loss, and E. V. Sukhorukov, Phys. Rev. B **61**, R16303 (2000).