Dual computational basis qubit in semiconductor heterostructures

M. J. Gilbert,[a] R. Akis, and D. K. Ferry
Department of Electrical Engineering and Center for Solid State Electronics Research, Arizona State University, Tempe, Arizona 85287-5706

(Received 12 November 2002; accepted 19 April 2003)

Advances in quantum computing have revealed computing capabilities that threaten to render many of the public encryption codes useless against the hacking potential for a quantum-mechanical-based computing system. This potential forces the study of viable methods to keep vital information secure from third-party eavesdropping. In this letter, we propose a coupled electronic waveguide device to create a qubit with two computational bases. The characteristics we have obtained by simulating such devices suggest a possible way of implementing quantum cryptography in semiconductor device architectures. © *2003 American Institute of Physics.* [DOI: 10.1063/1.1599633]

Recently, quantum computing has received a great deal of focus as a means for replacing the traditional complementory metal–oxide–semiconductor architecture. This has been, in large part, due to the numerous attractive features that quantum computing offers. Of these features, the most popular is the ability to achieve very rapid computation speeds as compared with that of the classical computation.[1,2] However, in addition to simply being a method to speed the computation, quantum computing offers tremendous promise in areas that are classically unrealizable or impractical, such as quantum teleportation[3] and the factorization of very large numbers into requisite primes.[4] If realized, the latter ability, which exploits the massive parallelism of quantum computation, would render all of the current public codes vulnerable to eavesdropping. As a means of possibly circumventing this problem, we propose a semiconductor qubit[5] possessing two separate computational bases to be implemented in an InGaAs/InAs heterostructure. The device in question, which we numerically simulate, utilizes a coupled electron waveguide structure with an embedded quantum point contact (QPC) to provide bit encoding both through the location of the electron density and through the manipulation of the spin of the electron. Such a qubit, if realized, would be ideal for application to secure communications.

Thus far, there have been several implementations offered to solve the problem of quantum hacking, but the majority of these implementations have revolved around the use of differing polarizations of photons or through nuclear magnetic resonance[6–9] to transmit bits based on different quantum keys, or protocols.[10–12] Nonetheless, the ability to implement a cryptographical system in a solid-state setting has not been offered previously. The ability to encrypt transmissions in a semiconductor setting is vital in that it would enable us to integrate the cryptography scheme into existing semiconductor chips to provide secure transmissions of data.

The structure we propose would utilize split metal gates over an InGaAs/InAs heterostructure. The enhanced Landé g-factor that InAs possesses (-15), as compared to, say, GaAs (which has a g-factor of only -0.44), would allow this device to filter the electrons according to spin with a reduced magnetic field. The gates would be patterned and biased to create two parallel waveguides, separated by an electrostatic potential barrier, except where they are coupled via a tunneling region. In our simulation, we assume the top waveguide has a uniform width of 35 nm, with a small QPC of width 35 nm and length 20 nm embedded in the left-hand side of the input waveguide. The bottom waveguide is narrowed at the source end to 25 nm and then widens to a width of 45 nm after the coupling region. The potential barrier is sufficiently high to prevent any leakage from the input waveguide to the output waveguide and assures all transfer of electron density from the input to the output occurs in the coupling region. The Fermi energy in the structure is chosen to be 9 meV, which corresponds to a carrier density of $9\times 10^{10}\ \text{cm}^{-2}$. This Fermi energy is chosen so that only one mode is excited in the input waveguide of the structure. The particular dimensions of the waveguide structure can be easily scaled as long as the constraints mentioned are honored. The quantum simulation of this system is performed on a finite difference grid using a mode-matching variant, which

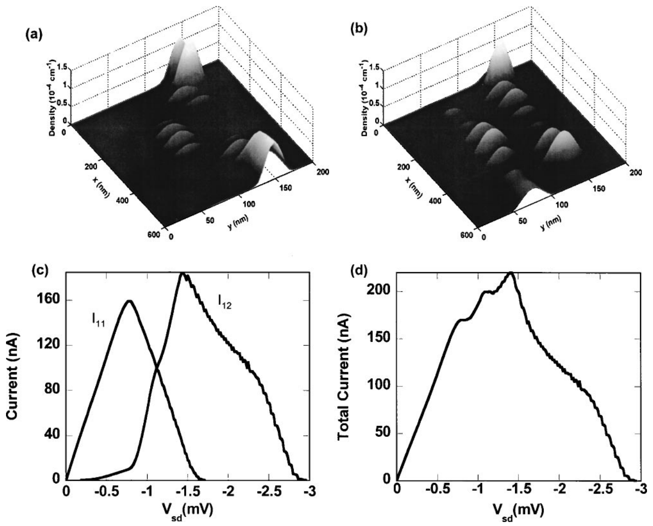

FIG. 1. Effects of electrical bias. (a) Electron density when the electrical bias is $V_{\text{sd}}=-0.78$ mV, with $T=0.7$ K, which corresponds to a maximal transmitted current present in the input waveguide (I_{11}). (b) Electron density when the electrical bias is $V_{\text{sd}}=-1.64$ mV, with $T=0.7$ K, which corresponds to a maximal current in the output waveguide (I_{12}). (c) I_{11} and I_{12} plotted against varying electric bias to show the profile of the individual transmissions. (d) Total current flowing in the device plotted against varying electric bias to show the profile of the total transmission through the device.

[a] Electronic mail: matthew.gilbert@asu.edu

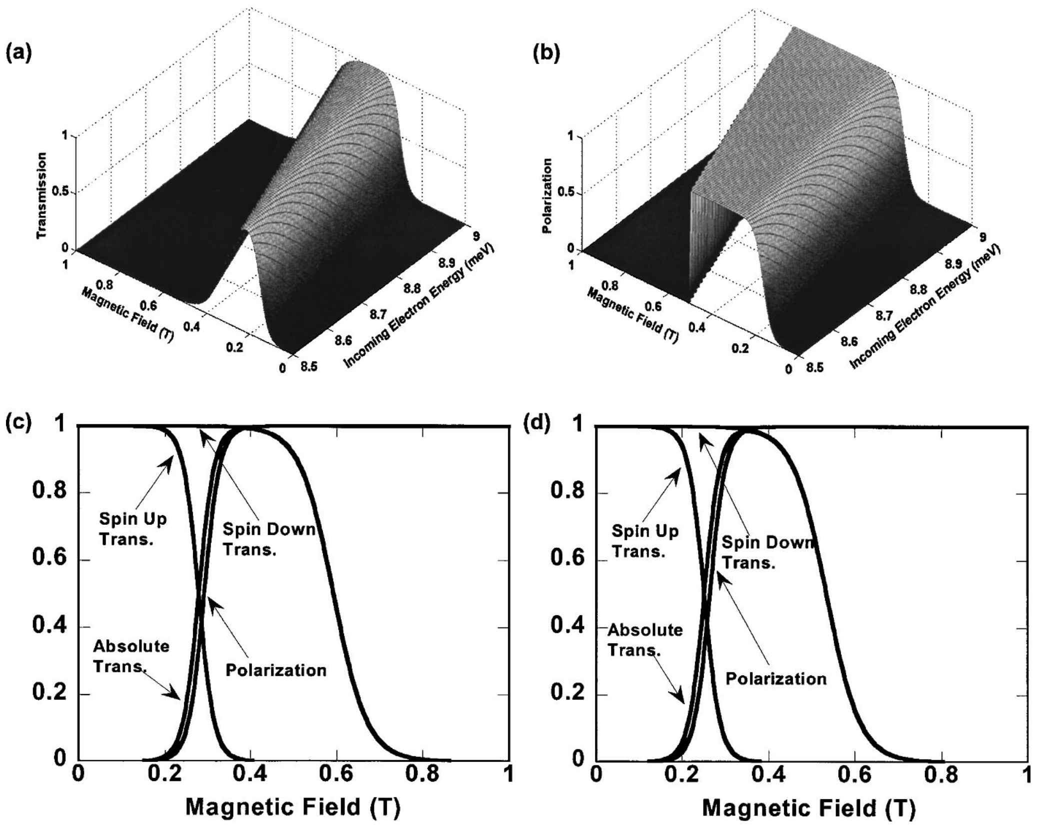

FIG. 2. Operation of the QPC as a spin filter. (a) Surface plot of the absolute transmission probability ($T_{\mathrm{abs}} = T\downarrow - T\uparrow$) for a QPC of potential profile $V(x,y) = V_0 - \frac{1}{2} m^* \omega_x^2 x^2 + \frac{1}{2} m^* \omega_y^2 y^2$ with $V_0 = 8.0$ MeV, $\hbar\omega_x = 0.1$ MeV, $\hbar\omega_y = 0.05$ MeV, and $T = 0.7$ K, with varying incoming electron energy and magnetic field. (b) Surface plot of the polarization $[P = (T\downarrow - T\uparrow)/(T\downarrow + T\uparrow)]$ of the incoming electrons plotted against varying energy and magnetic field. (c) Filtration characteristics for electrons with incident energy corresponding to $V_{\mathrm{sd}} = -0.78$ mV. (d) Filtration characteristics for electrons with incident energy corresponding to $V_{\mathrm{sd}} = -1.64$ mV.

utilizes a cascade of scattering matrices.[13] The grid spacing used was 5 nm. To make the simulation more realistic, we have included thermal effects and Zeeman splitting in the system.

With the structure defined, we must define the protocol under which our system operates. The protocol we use is a variation of the B92 protocol,[10] and it operates in the following manner. The sender randomly chooses numbers a and b, where a corresponds to the location of the density, "0" or "1" (upper or lower waveguide), and b corresponds to the polarization of the propagating density, "0" or "1" (unpolarized or spin down). Thus, as the electron density passes the input end of the device into the tunnel region, we have four possible states for the electrons: $\psi = (|0\uparrow\rangle + |0\downarrow\rangle)/\sqrt{2}(a = 0, b = 0)$, $|0\downarrow\rangle(a = 0, b = 1)$, $(|1\uparrow\rangle + |1\downarrow\rangle)/\sqrt{2}(a = 1, b = 0)$, or $|1\downarrow\rangle(a = 1, b = 1)$. It should be noted that the values of a and b, need not be randomly chosen. The values of a and b are randomly chosen only if the device is going to be used in a cryptographical sense, where randomness is key. However, the device may simply be operated as a simple qubit with two computational bases. This allows for greater flexibility as one qubit could conceivably now operate as two. The location of the electron density could be used as one qubit, while at the same time the spin of the arriving electron density could function as a completely noninteracting second qubit. Nonetheless, the device characteristics presented may be applied to cryptography in the following manner: the receiver then chooses a measurement basis and records the outcome of his measurement, his measurement basis, and the waveguide in which the electron density arrived. The measurement basis and the waveguide in which the electron density arrived are then publicly communicated to the sender from the receiver to reconcile and throw away incorrect measurements on the arriving density. With a protocol in place, we break up the system into three operational areas to explain the operation of the device for both cyptographical and normal modes of operation: input region, public region, and output region.

The input end of the device is defined as the section of the system that is to the left of the start of the coupling region. At the input end of our device, we have the input waveguide, the output waveguide on the bottom, and the QPC. We assume that the mode that is propagating at the input end of the device consists of mixed spins, or $\psi = (\alpha|\uparrow\rangle + \beta|\downarrow\rangle)/\sqrt{2}$ where α and β are real numbers. To send a message, the sender varies the electrical bias applied to the system and the magnetic field applied to the QPC. The applied bias is used to control in which waveguide the electron density arrives at the output end of the device and ultimately determines the value of a. Lower biases are used to send the electron density to the input waveguide $(a = 0)$ and higher biases are used to send the electron density to the output waveguide $(a = 1)$.[14] This varying of the position of the electron density provides the sender with one basis upon which he may send his bits. Nonetheless, in order to have a cryptographical key or a dual-mode qubit, we must have at least two bases present in the system. To form the second nonorthogonal basis, we use the QPC with a magnetic field

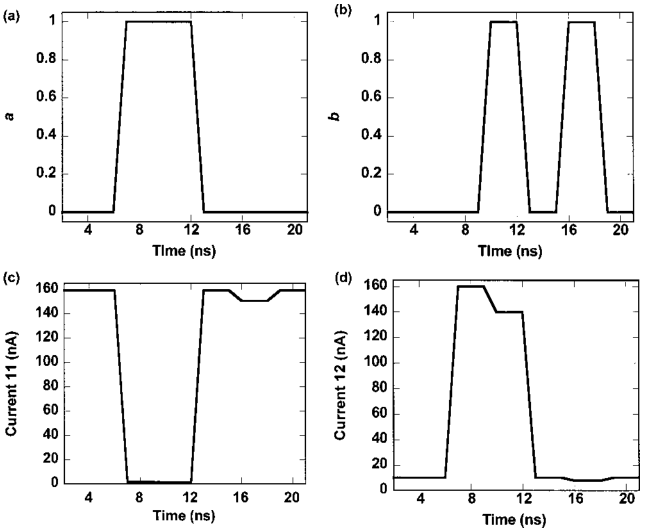

FIG. 3. Simulated operation of the cryptographical device. (a) Plot of the random variable *a* which controls the ultimate location of the electron density as a function time. (b) Plot of the random variable *b* which controls the polarization of the electron density as a function time. (c) Plot of the current flowing in the input waveguide at the receiver end of the device as a function of time. In the simulation, we have assumed that both the applied bias and the magnetic field may be switched on a time scale of picoseconds. Further, we also assume that using a hold time of 3 ns gives enough time for the mode to propagate from the sender to the receiver. We can see that the spin-polarized current values do not differ much from the nonpolarized values, thereby giving eavesdroppers very little additional information as to the value of b. (d) Plot of the current flowing in the output waveguide at the receiver end of the device as a function of time. While at the I_{11} maximum the current in the output waveguide does not vanish, the transmission probabilities and, therefore, the current, are greatly reduced. While it is ideal for I_{12} to disappear at the I_{11} maximum, the device operation, due to the definition of the protocol, is not affected.

applied to polarize the spins of the incoming mode,[15] which ultimately determines the value of b. A high value of magnetic field will polarize the density when $a=0$ and a low magnetic field polarizes the density when $a=1$. We assume that at the input end of the device, the sender controls the operation of the QPC and the electrical bias that is applied to the system, and that the values of these are known only by the sender. Therefore, at the input end, the sender may choose to send any of the four states based on the values of the applied bias, as shown in Fig. 1, and the local magnetic field in the QPC, as shown Fig. 2.

As the mode passes through the QPC and assumes one of the four possible states, it enters the public region of the device, which consists of the coupling region between the input and output waveguides. In this region, the system is open to eavesdropping from third parties. Nevertheless, this is a rather futile task in that not only must the third party choose one of the four possible bases in which to measure the transmitted bit, but while the electron density interacts with the output waveguide, it has not yet revealed its final destination to be the input or the output waveguide, thereby yielding the eavesdropper no insight as to which basis to choose. Further, the detection of the eavesdropper is quite simple, as the measurement made in the public section of the system, no matter how nonintrusive,[16] will corrupt the transmission coefficients by forcing the wavefunction into a state that does not correspond to the intended state, thus resulting in bit transmission errors detectable by the receiver.

With the mode passing the public area of the system, it enters the output end of the device. The output end of the device consists of the input and output waveguides. As the electron density arrives in either the input or the output waveguide with its given polarization, the receiver chooses a value for a by measuring either the input or output waveguide. At the same time, the receiver must also choose to measure either the mixed electron spin basis or the polarized spin basis to determine the value of b from the eigenstate of the measurement basis. It should be noted that in the output region, we do not need to assume that we are free from eavesdropping. This is true because the wavefunction is still in one of the four possible states, as in the public section of the device. Therefore, the chances of the key being deciphered are still quite low. Once the basis has been chosen and the current is measured, the receiver records the waveguide in which the electron density has arrived, the basis in which the measurement has been made, and the result of the measurement, as shown in Fig. 3. Information is publicly reconciled without revealing the result of the measurement, and thus, at the end of the reconciliation, the sender and the receiver have the same bit set and the message has been successfully transmitted. Moreover, Fig. 3 shows that if both a and b were set and then varied, we would still have a viable device.

In summary, we propose a semiconductor qubit that has two nonorthogonal computational bases. Such a qubit clearly has potential applications in cryptographic systems that are compatible with semiconductor integration. The proposed protocol couples spin polarization with waveguide switching to achieve the needed encryption for the secure transmission of bits.

The authors wish to thank Lucian Shifren for helpful discussions. This work is supported by the Office of Naval Research.

[1] P. Benioff, J. Stat. Phys. **22**, 495 (1980).
[2] D. Deutsch, Phys. Rev. Lett. **48**, 286 (1982).
[3] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wooters, Phys. Rev. Lett. **70**, 1895 (1993).
[4] P. W. Shor, *Proceedings of the 35th Annual Symposium on the Foundations of Computational Science* (IEEE Comp. Soc. Press, Los Alamitos, CA, 1994), p. 124.
[5] I. L. Chung and M. A. Nielsen, *Quantum Computing and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[6] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. W. Leung, Proc. R. Soc. London, Ser. A **454**, 447 (1998).
[7] C. H. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[8] A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1996).
[9] H. Zbindin, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, Electron. Lett. **33**, 586 (1997).
[10] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[11] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984) p. 175.
[12] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[13] T. Usuki, M. Saito, M. Takatsu, R. A. Kiehl, and N. Yokoyama, Phys. Rev. B **52**, 8244 (1995).
[14] M. J. Gilbert, R. Akis, and D. K. Ferry, Appl. Phys. Lett. **81**, 4284 (2002).
[15] M. J. Gilbert and J. P. Bird, Appl. Phys. Lett. **77**, 1050 (2000).
[16] O. Alter and Y. Yamamoto, Phys. Rev. Lett. **74**, 4106 (1995).