$N - m$ pairs must be singlets. Instead of computing the fidelity for the remaining $N - m$ pairs to be $N - m$ singlets, let us compute the fidelity for the original N pairs to be N singlets. This will give us a good enough bound on the fidelity. With any cheating strategy against the quantum verification scheme by Eve, let p_1 be the total probability for the state of the N pairs to be N singlets under the measurement along the Bell basis. The case of N singlets, which happens with a probability p_1, will automatically pass the verification test. This case is perfectly fine and secure. What about the other case? Upon a random-hashing verification scheme that sacrifices m pairs, the other case (which happens with probability $1 - p_1$) will pass an m-round random-hashing verification test with a conditional probability of, at most, 2^{-m}. Therefore, the probability that a strategy passes the verification test is given by

$$P(\text{passing}) \leq p_1 + 2^{-m}(1 - p_1) \leq p_1 + 2^{-m} \quad (5)$$

Eve would be most interested in a cheating strategy that passes the test with a nonnegligible probability (say at least 2^{-r}, where we assume that $0 < r \ll m$). Therefore, we demand that the probability

$$P(\text{passing}) \geq 2^{-r} \quad (6)$$

Combining Eqs. 5 and 6, we find that

$$p_1 + 2^{-m} \geq 2^{-r}$$

$$p_1 \geq 2^{-r}[1 - 2^{-(m-r)}] \quad (7)$$

Conditional on passing the verification test, the fidelity of the N pairs as singlets is given by

$$F' \geq \frac{p_1}{p_1 + 2^{-m}} \geq \frac{2^{-r}[1 - 2^{-(m-r)}]}{2^{-r}[1 - 2^{-(m-r)}] + 2^{-m}} = [1 - 2^{-(m-r)}] \quad (8)$$

where Eq. 7 and the fact that $p_1/(p_1 + 2^{-m})$ is an increasing function of p_1 have been used. By choosing a value of m that is substantially larger than r, the conditional fidelity can be made very close to 1. Therefore, given any parameter r, one can increase the conditional fidelity in Eq. 8 by increasing the number m of random parities computed. In summary, consider any eavesdropping strategy that passes an m-round random-hashing verification scheme with a probability of at least 2^{-r} (where $m \gg r > 0$. From Eq. 8, upon passing the test, the conditional fidelity of the N pairs as N singlets is at least $1 - 2^{-(m-r)}$. From (*28*), this implies that Eve's information is exponentially small in $m - r$, more precisely, $2^{-c} + O(2^{-2(m-r)})$, where $c = m - r - \log_2[2(N - m) + m - r + 1/(\log_e 2)]$.

37. R. B. Griffiths and C.-S. Niu, *Phys. Rev. Lett.* **76**, 3228 (1996).
38. Our classical argument applies to the N-Bell basis, whose basis vectors are highly entangled. It is perhaps surprising at first that the coarse-grained probabilities of a quantum mechanical experiment involving only local operations and classical communication can have a classical interpretation with respect to such a highly nonlocal basis. Put in another way, given the lesson from the EPR paradox, it is perhaps surprising that classical arguments can still be used to demonstrate that two distantly separated quantum subsystems are, in fact, highly quantum (that is, highly entangled).
39. C. A. Fuchs, *Fortschr. Phys.* **46**, 535 (1998), and references cited therein.
40. Incidentally, our result also proves the security of quantum money proposed by Wiesner (*1*). Indeed, the proof for our second example can be used to derive a probabilistic bound on the entropy of the combined system consisting of the quantum banknote and the bank. Consequently, any double-spending strategy will almost surely fail in the verification step (as in BB84) done by the bank because this entropy will no longer be close to zero.
41. J. Smolin, personal communication.

42. H.-K. Lo particularly thanks A. Ekert for pressing him to investigate the security of QKD. We thank numerous colleagues, including C. H. Bennett, G. Brassard, I. Chuang, D. P. DiVincenzo, C. A. Fuchs, N. Gisin, D. Gottesman, E. Knill, D. W. C. Leung, N. Lütkenhaus, D. Mayers, S. Popescu, J. Preskill, J. Smolin, T. Spiller, A. Steane, and A. C.-C. Yao for invaluable conversations and suggestions. Many helpful suggestions from an anonymous referee are gratefully acknowledged. H. F. Chau is supported by Hong Kong Government RGC grant HKU 7095/97P.

23 July 1998; accepted 26 January 1999

REPORTS

The Effect of Spin Splitting on the Metallic Behavior of a Two-Dimensional System

S. J. Papadakis,[1]* E. P. De Poortere,[1] H. C. Manoharan,[1]† M. Shayegan,[1] R. Winkler[2]

Experiments on a constant-density two-dimensional hole system in a gallium arsenide quantum well revealed that the metallic behavior observed in the zero–magnetic-field temperature dependence of the resistivity depends on the symmetry of the confinement potential and the resulting spin splitting of the valence band.

For many years, it was accepted that there could be no metallic phase in a disordered two-dimensional (2D) carrier system. This was due to the scaling arguments of Abrahams *et al.* (*1*) and the support of subsequent experiments (*2*). In the past few years, however, experiments on high-quality 2D systems have provided us with reason to revisit the question of whether or not a metallic phase in a 2D system can exist (*3–9*). Early temperature-dependence data from high-mobility Si metal oxide semiconductor field-effect transistors (MOSFETs) showed a decrease in resistivity as the temperature T was reduced below 2 K (*3*). This metallic behavior is the opposite of the expected insulating behavior in which the resistivity should become infinite as T approaches zero. In addition, the behavior was not only metallic in a certain electron density range but also scaled with a single parameter as the density was reduced and as the sample became insulating, suggesting a true metal-to-insulator phase transition (*3*).

Since these experiments, the metallic behavior has been observed in Si MOSFETS (*3, 4*), SiGe quantum wells (*5, 6*), GaAs/AlGaAs heterostructures (*7, 8*), and AlAs quantum wells (*9*), demonstrating that there are still some unsolved puzzles in the fundamental nature of 2D carrier systems. Multiple mechanisms, including electron-electron interaction (*10*), spin splitting (*11*), and T dependence of traps (*12*), have been proposed as causes of the metallic behavior, but no clear model that fully describes this sizeable body of experimental data has emerged. The experiments reported here add to our understanding by demonstrating a correlation between the zero–magnetic-field spin splitting and the metallic behavior.

Spin splitting of carriers in a 2D system at a zero magnetic field occurs when there is spin-orbit interaction and an inversion asymmetry of the potential in which the carriers move (*13*). The energy bands are split into two spin subbands, which have different populations because their energies at any nonzero wave vector $\vec{k}$ are slightly different. The existence of these spin subbands has been well established both experimentally and theoretically (*13–18*).

Our experiments were performed on high-mobility 2D hole systems in GaAs quantum wells (QWs), which were chosen because they have a large intercarrier separation r_s (*19*), they have already shown metallic behavior (*7, 8*), and they exhibit a large and tunable spin splitting (*17*). In GaAs, the spin splitting arises from the inversion asymmetries of the zinc-blende crystal structure and of the potential used to confine the electrons to two dimensions. The asymmetry of the crystal structure is fixed, but the asymmetry of the confining potential, and therefore the spin splitting, can be changed by applying an $\vec{E}$ perpendicular to the 2D plane ($E_\perp$) using gates (*17*). We found that the spin splitting can be tuned while the density is kept constant and that the metallic behavior of the 2D

[1]Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA. [2]Institut für Technische Physik III, Universität Erlangen-Nürnberg, Staudtstrasse 7, D-91058 Erlangen, Germany.

*To whom correspondence should be addressed. E-mail: papadaks@el.princeton.edu

†Present address: IBM Research Division, Almaden Research Center, 650 Harry Road, San Jose, CA 95120, USA.

holes is related to the amount of observed spin splitting.

Our samples were QWs that were Si modulation doped, 200 Å wide, and grown by molecular beam epitaxy on the (311)A surface of an undoped GaAs substrate. Quantum wells grown on the (311) surface of GaAs exhibit a mobility anisotropy that is thought to be caused by anisotropic interface roughness scattering (*20*). Photolithography was used to pattern L-shaped Hall bars that allowed the simultaneous measurement of the resistivities along both the high-mobility [$\bar{2}$33] and low-mobility [01$\bar{1}$] directions. The samples had metal front and back gates that controlled the 2D hole density and $E_\perp$. Measurements were done in a dilution refrigerator at T from 0.7 K to 25 mK and in perpendicular magnetic fields B up to 16 T. We used the low-frequency lock-in technique, with a current of 10 nA, to measure the longitudinal (ρ) and Hall resistivities.

To measure the spin splitting, we examined the low-B ρ, or Shubnikov–de Haas (SdH), oscillations (*16–18*). The frequencies of these oscillations, when multiplied by the level degeneracy e/h (e is the electron charge and h is Planck's constant), give the spin-subband densities, which are a measure of the zero-B spin splitting. To tune the splitting, we set the front-gate (V_{fg}) and back-gate (V_{bg}) voltages and measured the resistivities as a function of B on both arms of the Hall bar. Then, at a small B, V_{fg} was increased, and the change in the hole density was noted. V_{bg} was then reduced to recover the original density. This procedure changes $E_\perp$ while maintaining the same density to within 1% and allows calculation of the change in $E_\perp$ from the way that the gates affect the density. These steps were repeated until we had probed the range of V_{fg} and V_{bg} that is accessible without causing gate leakage. This was done for two samples, which were from different wafers, at 2D hole densities of 2.3×10^{11} cm^{-2} ($r_s = 6.8$) and 3.3×10^{11} cm^{-2} ($r_s = 5.7$) (*19*). These densities place the samples well into the metallic regime (*7, 8*). The 25 mK mobilities of the two samples are 83 and 51 m^2 V^{-1} s^{-1} for the [$\bar{2}$33] direction and 72 and 33 m^2 V^{-1} s^{-1} for the [01$\bar{1}$] direction, respectively. The results from both samples are similar.

Some of the low-B ρ data are shown (Fig. 1A) at a density of 3.3×10^{11} cm^{-2} from both the low- and high-mobility directions for various sets of V_{fg} and V_{bg}. The top panel of Fig. 1A was taken with the sample at a large positive $E_\perp$ (~5000 V cm^{-1} pointing toward the front gate). $E_\perp$ is reduced in the second panel, nearly zero in the middle panel, and increasingly negative in the bottom two panels of Fig. 1A (it is about −6000 V cm^{-1} in the bottom panel). The frequencies f_{SdH} of the SdH oscillations were extracted by Fourier transforming the ρ versus B^{-1} data in the range below 0.9 T. The Fourier transforms of the low-mobility data (Fig. 1B) reveal how the spin splitting changes as $E_\perp$ is changed from positive, through zero, to negative. From the symmetry of the data in Fig. 2A, we estimate that $E_\perp = 0$ is near $V_{fg} = -0.5$ V.

The next part of the experiment involved measuring the T dependence of ρ at $B = 0$ from 25 mK to ~0.7 K. In the data from the low-mobility direction (Fig. 1C), the traces are separated vertically and displayed next to the corresponding Fourier transforms in Fig. 1B for clarity. Their ρ values at 25 mK and $B = 0$ (ρ_0) are shown on the y axis. The most striking feature is that the T dependence of the $B = 0$ resistivity is larger when the two f_{SdH} peaks are well separated and smaller when there is no separation. It is clear that the magnitude of the T dependence is correlated with that of the spin splitting. In order to characterize this data in a simple way, we plotted $\Delta\rho^T/\rho_0$, the fractional change in ρ from 25 mK to 0.67 K (Fig. 2B). Figure 2, A and B, clearly shows that ρ increases more strongly with T as the difference between the SdH frequencies (Δf_{SdH}) is increased. The same is true of the lower density sample. Additionally, $\Delta\rho^T/\rho_0$ is larger for lower density, consistent with previous experiments on the metallic behavior (*3–9*).

Finally, we attempted to more quantitatively determine what the T dependence would be in the limit of zero spin splitting. To this end, we have performed simulations with self-consistent subband calculations that have no adjustable parameters (*17*). They provide, for a given 2D hole density and $E_\perp$, both simulated SdH oscillations and the zero-B spin-subband population difference (Δp_s). Fourier transforms of the simulated SdH oscillations show peak positions that agree with those from the experimental data. Furthermore, whereas the sum of the f_{SdH}

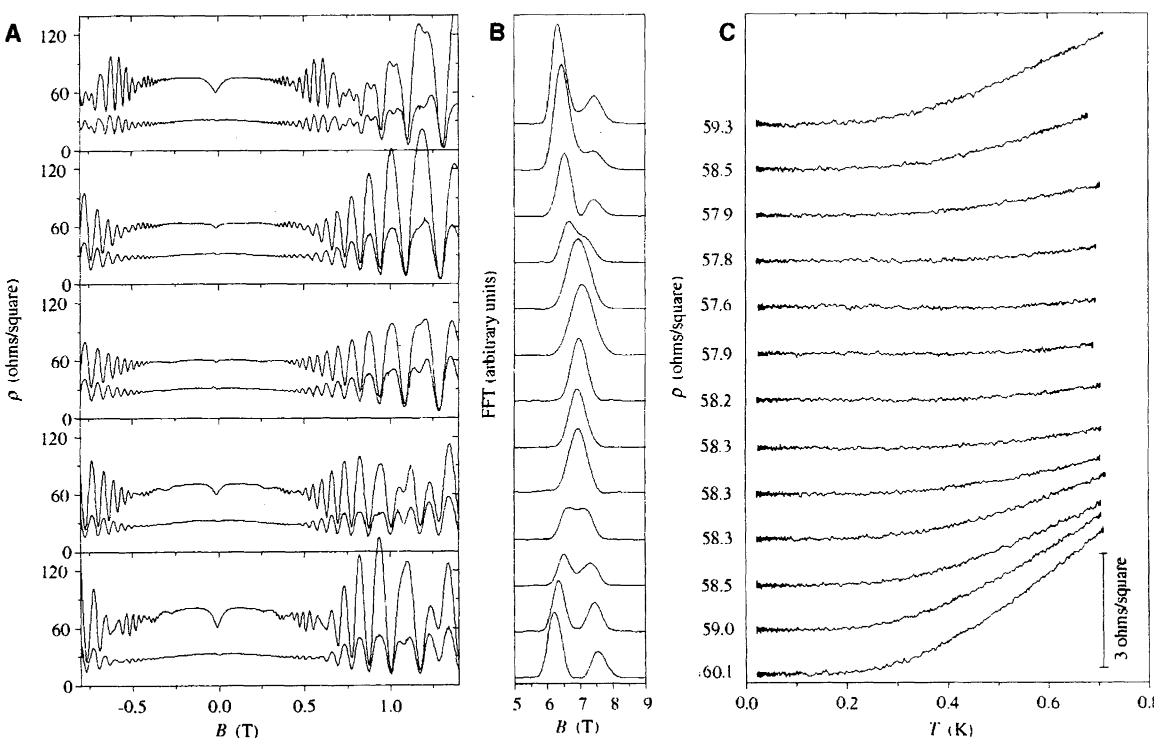

Fig. 1. (**A**) Magnetoresistance traces, all at a density of 3.3×10^{11} cm^{-2} but at different values of $E_\perp$. The data shown are from the low-mobility [01$\bar{1}$] (top trace in each panel) and high-mobility [$\bar{2}$33] (bottom trace in each panel) directions. (**B**) Fast Fourier transforms (FFT) of the SdH oscillations, showing that the spin splitting is being tuned through a minimum. (**C**) Temperature dependence of ρ for the low-mobility direction. The traces are shifted vertically for clarity, with the value of ρ at 25 mK listed along the y axis for each trace. Each trace of ρ versus T is aligned with its corresponding Fourier transform. Together, (B) and (C) show that the magnitudes of the spin splitting and the T dependence are related.

multiplied by e/h gives the total density, the calculations show that the Δf_{SdH} value underestimates the zero-B Δp_s at all $E_\perp$. In particular, the simulations predict a finite zero-B spin splitting at $E_\perp = 0$ (caused by the inversion asymmetry of the GaAs crystal structure), whereas for $|E_\perp| < 1000$ V cm^{-1}, the Fourier transforms of the simulated SdH oscillations and of the experimental data show only one peak. The measured $\Delta\rho^T/\rho_0$ were plotted versus the calculated Δp_s (Fig. 3) with the data for positive and negative $E_\perp$ separated on either side of the x-axis zero for clarity. These results suggest that $\Delta\rho^T/\rho_0$ would be zero or less than zero in the limit of zero spin splitting.

The data show that the magnitude of $\Delta\rho^T/\rho_0$ increases with the magnitude of $E_\perp$, which directly affects the amount of spin splitting. Mobility is also affected by $E_\perp$. However, as shown by the ρ_0 values on the y axis of Fig. 1C, the changes in mobility do not correlate with changes in $\Delta\rho^T/\rho_0$. For example, for three of the traces, ρ_0 remains steady at 58.3 ohms/square, but $\Delta\rho^T/\rho_0$ changes. Additionally, $\Delta\rho^T/\rho_0$ is large when the mobility is small, in contrast to the observation that the metallic behavior becomes more pronounced as the mobility is improved (*4*). Also, the dependence of mobility on $E_\perp$ varies from sample to sample and along different mobility directions within each sample (*21*). Thus, it is very unlikely that the mobility variation is causing the changes in $\Delta\rho^T/\rho_0$.

There are striking differences between the data along the low- and high-mobility directions that add a new twist to this problem.

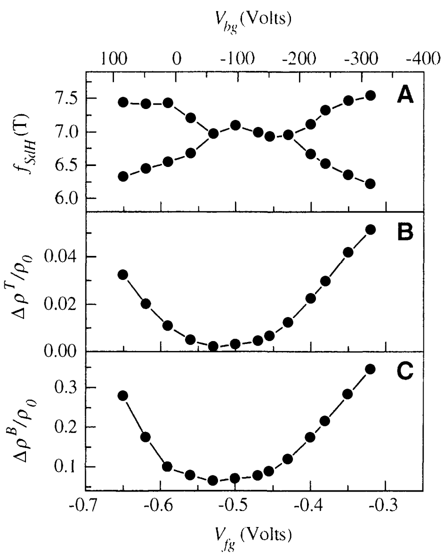

Fig. 2. (**A**) Measured SdH frequencies plotted as a function of V_{fg}. Each V_{fg} has a corresponding V_{bg} (top x axis) that is used to keep the density constant but to vary $E_\perp$. (**B**) $\Delta\rho^T/\rho_0$ versus V_{fg}. $\Delta\rho^T$ is the change in ρ from $T = 25$ mK to 0.67 K, and ρ_0 is ρ at 25 mK and $B = 0$ T. (**C**) $\Delta\rho^B/\rho_0$ versus V_{fg}. $\Delta\rho^B$ is the change in ρ from $B = 0$ to 0.1 T at 25 mK.

Whereas the behaviors with $E_\perp$ are qualitatively similar, $\Delta\rho^T/\rho_0$ is an order of magnitude smaller in the high-mobility direction. Additionally, the low-mobility direction ρ shows a strong positive magnetoresistance, which is not present in the high-mobility ρ, that saturates at ~0.1 T. Its magnitude at 25 mK, $(\Delta\rho^B/\rho_0) = [\rho(0.1\text{ T}) - \rho(0\text{ T})]/\rho_0$, was plotted (Fig. 2C) and is remarkably similar to $\Delta\rho^T/\rho_0$ in Fig. 2B, despite the different origins (B and T dependence). The difference in mobility for the two directions is thought to come from an anisotropic interface roughness scattering that is due to the interface morphology [see (*20*) and references therein]. On the other hand, the Fourier transforms of the SdH oscillations show that the spin splitting is the same in both directions, so it is clear that the changes in $\Delta\rho^B/\rho_0$ and $\Delta\rho^T/\rho_0$ are not due to spin splitting alone. It is possible that the directional differences in the B and T dependencies of ρ are due to an interplay between the applied B field or the spin splitting and the anisotropic scattering mechanism in the sample. The precise nature of this interplay remains to be discovered. These observations point to the subtlety of the physics behind the metallic behavior in this system.

We observed that the magnitude of the T dependence of the resistivity (the metallic behavior) increases with the magnitude of the spin splitting. Previous experiments in applied B fields have provided evidence that the spin of the carriers plays an important role in the metallic behavior. However, in these experiments, the B field, which increases the spin splitting, quenches the metallic state (*8, 22*). This inconsistency is surprising, and we surmise that, in relation to the metallic behavior, there is some fundamental difference between the zero-B spin splitting, which is caused by the GaAs band structure and the confinement potential, and the nonzero-B spin splitting, which is the difference in energy between carriers with spins parallel and antiparallel to the applied B field (*23*). Furthermore, our results show a complication in experiments that examined the dependence of the metallic behavior on the carrier density: The spin splitting was changed as the density was

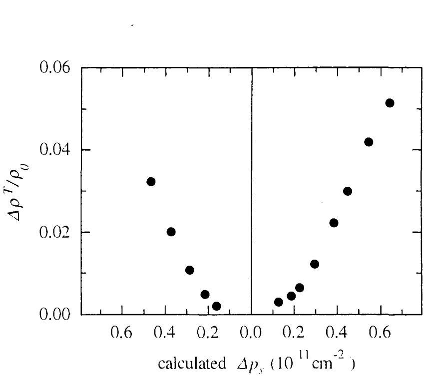

Fig. 3. $\Delta\rho^T/\rho_0$ from the high-density sample plotted versus the calculated zero-B population difference of the spin subbands.

changed (*3–9*). Recognition of the fact that the zero-B spin splitting is important should help untangle the causes of this unexpected phenomenon. Finally, we note that there are substantial differences between the low- and high-mobility direction data which have been overlooked in previous experiments on GaAs 2D holes. These differences may also provide clues to the nature of the metallic behavior.

References and Notes

1. E. Abrahams *et al.*, *Phys. Rev. Lett.* **42**, 673 (1979).
2. D. J. Bishop, D. C. Tsui, R. C. Dynes, *ibid.* **44**, 5737 (1980).
3. S. V. Kravchenko, G. V. Kravchenko, J. E. Furneaux, *Phys. Rev. B* **50**, 8039 (1994); S. V. Kravchenko *et al.*, *ibid.* **51**, 7038 (1995); S. V. Kravchenko *et al.*, *Phys. Rev. Lett.* **77**, 4938 (1996).
4. D. Popović, A. B. Fowler, S. Washburn, *Phys. Rev. Lett.* **79**, 1543 (1997).
5. P. T. Coleridge *et al.*, *Phys. Rev. B* **56**, R12764 (1997).
6. J. Lam *et al.*, *ibid.*, p. R12741.
7. Y. Hanein *et al.*, *Phys. Rev. Lett.* **80**, 1288 (1998).
8. M. Y. Simmons *et al.*, *ibid.*, p. 1292.
9. S. J. Papadakis and M. Shayegan, *Phys. Rev. B* **57**, R15068 (1998).
10. V. Dobrosavljević *et al.*, *Phys. Rev. Lett.* **79**, 455 (1997).
11. V. M. Pudalov, *JETP Lett.* (Engl. transl.) **66**, 175 (1997) [translation from *Pis'ma Zh. Eksp. Teor. Fiz.* **66**, 168 (1997)].
12. B. L. Altshuler and D. Maslov, *Phys. Rev. Lett.* **82**, 145 (1999).
13. Yu. A. Bychkov and E. I. Rashba, *JETP Lett.* (Engl. transl.) **39**, 78 (1984) [translation from *Pis'ma Zh. Eksp. Teor. Fiz.* **39**, 66 (1984)]. For a review, see U. Rössler, F. Malcher, G. Lommer, in *High Magnetic Fields in Semiconductor Physics II*, vol. 87 of *Springer Series in Solid State Sciences*, G. Landwehr, Ed. (Springer, Berlin, 1989), pp. 376–385.
14. B. Jusserand *et al.*, *Phys. Rev. B* **51**, 4707 (1995).
15. P. D. Dresselhaus *et al.*, *Phys. Rev. Lett.* **68**, 106 (1992).
16. J. P. Eisenstein *et al.*, *ibid.* **53**, 2579 (1984); B. Das *et al.*, *Phys. Rev. B* **39**, 1411 (1989); M. Schultz *et al.*, *Semicond. Sci. Technol.* **11**, 1168 (1996); J. Nitta, T. Akazaki, H. Takayanaga, T. Enoki, *Phys. Rev. Lett.* **78**, 1335 (1997).
17. J. P. Lu *et al.*, *Phys. Rev. Lett.* **81**, 1282 (1998).
18. K. Muraki and Y. Hirayama, *Physica B* **249**, 65 (1998).
19. The importance of carrier interaction is characterized by the parameter r_s. It is the average intercarrier separation in units of the effective Bohr radius. We used a GaAs dielectric constant of 13 and an effective hole mass of $0.4m_e$, deduced from cyclotron resonance measurements on similar samples [K. Hirakawa *et al.*, *Phys. Rev. B* **47**, 4076 (1993)].
20. J. J. Heremans *et al.*, *J. Appl. Phys.* **76**, 1980 (1994).
21. The behavior of the mobility with $E_\perp$ depends on the details of the disorder at the QW interfaces and is therefore expected to be different from one sample to the next. Furthermore, one would expect, as we observed, a lower mobility when the QW is asymmetric because the carrier wave function is pushed toward one of the interfaces, which are invariably somewhat disordered.
22. V. M. Pudalov *et al.*, *JETP Lett.* (Engl. transl.) **65**, 932 (1997) [translation from *Pis'ma Zh. Eksp. Teor. Fiz.* **65**, 168 (1997)]; D. Simonian *et al.*, *Phys. Rev. Lett.* **79**, 2304 (1997); S. V. Kravchenko *et al.*, *Phys. Rev. B* **58**, 3553 (1998).
23. The zero-B spin splitting is caused by spin-orbit interaction involving the carrier's momentum and the electrical potential that it is traveling through. In contrast, the nonzero-B spin splitting (Zeeman splitting) is caused by an applied external magnetic field.

24. We thank J. Yoon and B. Altshuler for useful discussions. This work was funded by NSF and the Army Research Office.

9 December 1998; accepted 19 February 1999