REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE 2 December 2001	3. REPORT TYPE AND DATES COVERED Final Rept. 1 August 1998-1 August. 2001

4. TITLE AND SUBTITLE
Quantum Information Processing

5. FUNDING NUMBERS
DAAG55-98-C-0041

6. AUTHOR(S)
David P. DiVincenzo
Charles H. Bennett

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
IBM Corp., T. J. Watson Research Center
PO Box 218, Yorktown Heights, NY 10598

8. PERFORMING ORGANIZATION REPORT NUMBER
4

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT	12 b. DISTRIBUTION CODE
Approved for public release; distribution unlimited.	

13. ABSTRACT (Maximum 200 words)

We have made progress on many fronts on the understanding and characterization of entanglement. Various new forms of bound (i.e. undistillable) entanglement have been introduced, as part of our work on unextendible product states. Cases of "superactivation" of bound entanglement, in which two different bound entangled states, when joined, produce distillable entanglement, have been established for four-party states and have been conjectured for bipartite states. These results show that the distillable entanglement is neither additive nor convex -- this achieves one of the major three year goals of this project. An explicit formula for the entanglement of formation was found for all isotropic mixed states. We discovered and characterized "remote state preparation", a generalization of quantum entanglement in which the transmitted quantum state is known to Alice. Very recently, with A. Winter, a new, more efficient protocol for RSP has been discovered.

We have continued to study many ideas for the simplication of the Kane approach to quantum computing, with the replacement of electron spin for nuclear spin. Important simplifications over the currently published device designs will be possible. We have worked out a scheme for the implementation of quantum computing, builing on the theory of decoherence-free subspaces, that uses only the Heisenberg exchange interaction, or only the XY interaction. We have provided detailed calculations of how g-factor engineering could be realized in III-V semiconductor heterostructures. We have shown how to ameliorate the effects of spin orbit interaction in quantum-dot qubits. We have begun master-equation modeling of superconducting qubits.

14. SUBJECT TERMS	15. NUMBER OF PAGES
	16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT	18. SECURITY CLASSIFICATION ON THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	**UNCLASSIFIED**	**UNCLASSIFIED**	**UL**

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used for announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to ***stay within the lines*** to meet ***optical scanning requirements.***

Block 1. Agency Use Only (Leave blank)

Block 2. Report Date. Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, and volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s) project number(s), task number(s), and work unit number(s). Use the following labels:

C - Contract	**PR** - Project
G - Grant	**TA** - Task
PE - Program Element	**WU** - Work Unit Accession No.

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es) Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. (*if known)*

Block 11. Supplementary Notes. Enter information not included elsewhere such as; prepared in cooperation with....; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NORFORN, REL, ITAR).

DOD - See DoDD 4230.25, "Distribution Statements on Technical Documents."
DOE - See authorities.
NASA - See Handbook NHB 2200.2.
NTIS - Leave blank.

Block 12b. Distribution Code.

DOD - Leave Blank
DOE - Enter DOE distribution categories from the Standard Distribution for unclassified Scientific and Technical Reports
NASA - Leave Blank.
NTIS - Leave Blank.

Block 13. Abstract. Include a brief (*Maximum 200 words)* factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subject in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code (NTIS *only*).

Block 17. - 19. Security Classifications. Self-explanatory. Enter U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (Unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

REPORT DOCUMENTATION PAGE (SF298)
(Continuation Sheet)

I. List of Most Significant Manuscripts Submitted or Published:

- G. Burkard, D. Loss, and D. DiVincenzo, "Coupled quantum dots as quantum gates," Phys. Rev. B 59, 2070 (1999).
- G. Burkard, D. Loss, D. P. DiVincenzo, and J. A. Smolin, "Physical optimization of quantum error correction circuits," Phys. Rev. B 60, 11404 (1999).
- D. P. DiVincenzo and D. Loss, "Quantum computers and quantum coherence," J. Mag. Magn. Matl. 200, 202 (1999).
- B. M. Terhal, I. L. Chuang, D. P. DiVincenzo, M. Grassl, and J. A. Smolin, "Simulating quantum operations with mixed environments," Phys. Rev. A 60, 881 (1999).
- C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, "Quantum nonlocality without entanglement," Phys. Rev. A 59, 1070 (1999).
- C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, "Unextendible product bases and bound entanglement," Phys. Rev. Lett. 82, 5385 (1999).
- A. Imamoglu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small, "Quantum Information processing using quantum dot spins and cavity QED," Phys. Rev. Lett. 83, 4204 (1999).
- D. P. DiVincenzo, D. Bacon, J. Kempe, G. Burkard, and K. B. Whaley, "Universal quantum computation with the exchange interaction," Nature 408, 339-342 (2000).**
- C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, “Exact and asymptotic measures of multipartite pure state entanglement,” quant-ph/9908073, Phys. Rev. A 63, 012307 (2001). **
- D. P. DiVincenzo, "The physical implementation of quantum computation," quant-ph/002077, Fort. der Phys. 48, 771-784 (2000).**
- C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, B. M. Terhal, and W. K. Wootters, "Remote state preparation," quant-ph/0006044, Physical Review Letters 87, 077902 (2001).**
- R. Vrijen, E. Yablonovich, K. Wang, H.-W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. P. DiVincenzo, “Electron spin resonance transistors for quantum computing in silicon-germanium heterostructures,” quant-ph/9905096, Phys. Rev. A 62, 012306 (2000).**
- D. P. DiVincenzo and B. M. Terhal, "Product Bases in Quantum Information Theory", quant-ph/0008055, to be published in Proceedings of the XIII International Congress on Mathematical Physics.**
- D. P. DiVincenzo, "Prospects for Quantum Computing," IEDM 2000 Technical Digest, 12-15.**
- E. N. Maneva and J. A. Smolin, "Improved two-party and multi-party purification protocols," quant-ph/0003099.**
- D. P. DiVincenzo, B. M. Terhal, and A. V. Thapliyal, “Optimal decompositions of barely separable states,” quant-ph/9904005, J. Mod. Optics 47, 377-385 (2000).**
- Debbie W. Leung, "Quantum Vernam Cipher," quant-ph/0012077.**
- D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, “Unextendible product bases, uncompletable product bases, and bound entanglement,” quant-ph/9908070, accepted by Commun. Math Phys.
- D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, “Evidence for bound entangled states with negative partial transpose,” quant-ph/9910026, Phys. Rev. A 61, 062312 (2000).**
- D. Bacon, A. M. Childs, I. L. Chuang, J. Kempe, D. Leung, and X. Zhou, "Universal simulation of Markovian quantum dynamics," quant-ph/0008070, Phys. Rev. A 64, 062302 (2001).
- D. P. DiVincenzo, G. Burkard, D. Loss, and E. V. Sukhorukov, “Quantum computation and spin electronics,” cond-mat/9911245, Chap. 27 of "Quantum Mesoscopic Phenomena and Mesoscopic Devices in Microelectronics", eds. I. O. Kulik and R. Eliatioglu (Kluwer, 2000).**
- B. M. Terhal and P. Horodecki, “A Schmidt number for density matrices,” quant-ph/9911117, Phys. Rev. A 61, 040301 (Rapid Communications) (2000).**
- A. M. Childs, I. L. Chuang, and D. W. Leung, "Realization of quantum process tomography in NMR," quant-ph/0012032.**
- P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Superactivation of bound entanglement," quant-ph/0005117.**
- C. H. Bennett and D. P. DiVincenzo, “Quantum Information and Computation” Nature (invited review) 404, 247-255 (2000).**
- J. A. Smolin, "Four-party unlockable bound entangled state," quant-ph/0001001, Phys. Rev. A 63, 032306 (2001).**
- P. W. Shor, J. A. Smolin, and B. M. Terhal, "Nonadditivity of bipartite distillable entanglement follows from a conjecture on bound entangled Werner states," Phys. Rev. Lett. 86, 2681 (2001).**
- B. M. Terhal and P. Horodecki, "Schmidt number for density matrices," Phys. Rev. A 61, 040301 (2000).**
- B. M. Terhal and K. G. H. Vollbrecht, "Entanglement of formation for isotropic states," Phys. Rev. Lett. 85, 2625 (2000).**
- P. M. Hayden, M. Horodecki, and B. M. Terhal, "The asymptotic entanglement cost of preparing a quantum state," quant-ph/0008134.**
- P. M. Hayden, B. M. Terhal, and A. Uhlmann, "On the LOCC classification of bipartite density matrices," quant-ph/0011095.**
- B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, "Hiding bits in Bell states," Phys. Rev. Lett. 86, 5807 (2001).
- N. E. Bonesteel, D. Stepanenko, and D. P. DiVincenzo, "Anisotropic spin exchange in pulsed quantum gates," Phys. Rev. Lett. 87, 207901 (2001).

- D. W. Leung, "Simulation and reversal of n-qubit Hamiltonians using Hadamard matrices," quant-ph/0107041.
- D. Bacon, J. Kempe, D. P. DiVincenzo, D. A. Lidar, and K. B. Whaley, "Encoded universality in physical implementations of a quantum computer," quant-ph/0102140.
- C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem," quant-ph/0106052.
- B. M. Terhal and D. P. DiVincenzo, "Classical simulations of noninteracting-fermion quantum circuits," quant-ph/0108010.
- M. Horodecki, P. Horodecki, R. Horodecki, D. W. Leung, and B. M. Terhal, "Classical capacity of a noiseless quantum channel assisted by noisy entanglement," quant-ph/0106080.
- J. Kempe, D. Bacon, D. P. DiVincenzo, and K. B. Whaley, "Encoded universaility from a single physical interaction," quant-ph/0112013.
- D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, "Quantum data hiding," quant-ph/0103098, accepted for publication by the IEEE Trans. Info. Theory.
- C. H. Bennett, J. I. Cirac, M. S. Leifer, D. W. Leung, N. Linden, S. Popescu, and G. Vidal, "Optimal simulation of two-qubit Hamiltonians using general local opoerations," quant-ph/0107035.

II. Scientific personnel: C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, B. M. Terhal (postdoc), D. Leung (postdoc).

IV. Scientific Progress:

Theory of Entanglement—We have made progress on many fronts on the understanding and characterization of entanglement. Various new forms of bound (i.e. undistillable) entanglement have been introduced, some obtained by our new proofs on the existence of various unextendible product bases. Cases of "superactivation" of bound entanglement, in which two different bound entangled states, when joined, produce distillable entanglement, have been established for four-party states and have been conjectured for bipartite states. These results show that the distillable entanglement is neither additive nor convex. New explicit protocols for bipartite and multipartite distillation were introduced. On the other side, we obtained new evidence in 2000 that the entanglement of formation is additive. An explicit formula for the entanglement of formation was found for all isotropic mixed states. Constraints were obtained on the cardinality of optimal (minimal entanglement) decompositions of mixed states. We introduced the Schmidt number as a new measure of entanglement.

Quantum Communication Protocols--We obtained three new results in this area in 2000. We discovered and characterized "remote state preparation", a generalization of quantum entanglement in which the transmitted quantum state is known to Alice. We have determined the minimal entanglement and classical-channel resources needed for RSP. We have introduced the "quantum Vernam cipher", in which shared entanglement is used to implement a securely recyclable one-time pad. And we have introduced various prototcols for the interconversion between different forms of quantum entanglement by local operations. In 2001 we finished a major work on the characterization of interconversions between states in a multipartite setting. There has been significant progress on entanglement-assisted channel capacity, and on the quantum reverse shannon theorem. We have also studied the simulation of one two-body Hamiltonian by another, a result which illustrates that their entangling power is a key parameter in these simulations. There has recently been exciting new results on remote state preparation, indicating, to our surprise, that standard quantum teleportation is *not* optimal for the transmission of states from Alice to Bob if Alice knows the quantum states. This represents a novel application of Winter's method of noiseless coding of POVM measurements.

Physical Implementations and Phenomenology— We have continued to study many ideas for the simplication of the Kane approach to quantum computing, with the replacement of electron spin for nuclear spin. Important simplifications over the currently published device designs will be possible. We have worked out a scheme for the implementation of quantum computing, builing on the theory of decoherence-free subspaces, that uses only the Heisenberg exchange interaction. We have provided detailed calculations of how g-factor engineering could be realized in III-V semiconductor heterostructures. We have investigated the spins of electrons in quantum wires as a new kind of flying qubit. New algorithms have been proposed

for the universal simulation of Markovian quantum dynamics. And, in NMR, a new protocol for quantum process tomography has been worked out. More recently, we have shown that linear Fermion optics can be efficiently simulated by a classical computer, which is quite different from the boson case (which gives the full power of quantum computation).
Cryptography--At the beginning of this program, we discovered "nonlocality without entanglement", which indicated that there would be a way to do secret sharing with joint quantum states. Recently we discovered how this could actually be accomplished ("secret sharing using Bell states") and we have made precise calculations of the level and kind of security achieved. In quantum-dot qubits, we have proposed a cavity QED implementation. This implementation has the XY interaction as the fundamental two-body interaction, and we have recently shown theoretically how this interaction (and the Heisenberg interaction, appropriate for the single-electron quantum dot quantum bit) can be used efficiently to implement quantum computation.
Reviews—We have written a couple of major overviews on the use of quantum computing tools for the solution of a wide range of information processing tasks, on the prospects for spin-based solid state quantum computation, and a general overview of the field (published in Nature) A plenary presentation and paper were given at the International Electron Device Meeting on the prospects for semiconductor quantum computers. A keynote article was written for a special issue on the physical implementation of quantum computation was written, reviewing the five criteria for the physical implementation of quantum computation.

Enclosure 2

MASTER COPY: PLEASE KEEP THIS "MEMORANDUM OF TRANSMITTAL" BLANK FOR REPRODUCTION PURPOSES. WHEN REPORTS ARE GENERATED UNDER THE ARO SPONSORSHIP, FORWARD A COMPLETED COPY OF THIS FORM WITH EACH REPORT SHIPMENT TO THE ARO. THIS WILL ASSURE PROPER IDENTIFICATION. NOT TO BE USED FOR INTERIM PROGRESS REPORTS; SEE PAGE 2 FOR INTERIM PROGRESS REPORT INSTRUCTIONS.

MEMORANDUM OF TRANSMITTAL

U.S. Army Research Office
ATTN: AMSRL-RO-RI (Hall)
P.O. Box 12211
Research Triangle Park, NC 27709-2211

☐ Reprint (Orig + 2 copies)
☐ Technical Report (Orig + 2 copies)
☐ Manuscript (1 copy)
☐ Final Progress Report (Orig + 2 copies)
☐ Related Materials, Abstracts, Theses (1 copy)

CONTRACT/GRANT NUMBER:

REPORT TITLE:

is forwarded for your information.

SUBMITTED FOR PUBLICATION TO (applicable only if report is manuscript):

Sincerely,