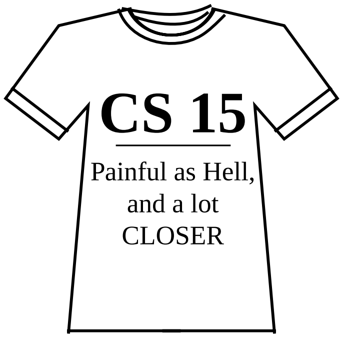
eration use e-mail, as we did when we were kids?" to more serious discussions on the nature of privacy in the world according to Oprah. The discussions ceased a few days later when the signs were replaced by a new set that read "Ed—I'll forgive you if you take me to the CS Department Picnic on August 29th. Pick me up at 1—Kerri" and the entire thing was found to be an advertising gimmick for our picnic. The perpetrator was Mark Oribello, astaff member and van Dam factotum extraordinaire! One of our grad students, Sonia Leach, was responsible for another nice piece of picnic advertising. This was a picnic scene on the wall opposite the mailboxes made up of cut-out paper caricatures of people in the department. The scene developed from day to day and had everyone in the department waiting to see who would appear next. Some of Sonia's impressions appear on this and the previous page.



Mike Shantzis, '84 BA, '86 MS, received an Academy Award for his work at Pixar on Disney's *Beauty and the Beast*.

conduit!

A publication of
The Computer Science Department
Brown University

Inquiries to: *conduit!*
Department of Computer Science
Box 1910, Brown University
Providence, RI 02912
FAX: 401-863-7657
PHONE: 401-863-7610
EMAIL: sjh@cs.brown.edu
WWW: http://www.cs.brown.edu/publications/conduit/

Suzi Howe
Editor-in-Chief

Katrina Avery
Editor

Jeff Coady
Technical Support

Department of Computer Science
Brown University
Box 1910, Providence, RI 02912

conduit!

Printed on recyled paper

Address changes welcomed

on Strategic Directions in Computing Research in Cambridge. He gave invited lectures at the eighth Canadian Conference on Computational Geometry in Ottawa, the Workshop on Orders, Algorithms and Applications, also in Ottawa, and SIAM Discrete Mathematics Conference in Baltimore.

Peter Wegner. Peter lectured all over Europe this summer—Oxford, Amsterdam, Pisa, and Linz. He is editor of the ACM 50th anniversary symposium on Strategic Directions in Computing that will be published in the December issue of *Computing Surveys*—check out http://www.medg.lcs.mit.edu/sdcr/). He is an editor of the forthcoming CRC Press *Handbook of Computer Science and Engineering* and author of the first and the last chapters of this ambitious 150-author, 3000-page overview of the field. He is chairman of the committee for awarding the new ACM Kanellakis Theory and Practice award, and welcomes nominations for this award, which are due November 1, 1996.

Stan Zdonik. Stan has been awarded a three-year NSF grant for his work on Analytical and Empirical Tools for Advanced Query Optimization. He gave the keynote talk at the British National Conference on Databases entitled 'Your Data May Be Where You Least Expect It: Dissemination-Based Information Systems.'

Friends gather with President Gregorian (center) and the University chaplain (right foreground) to plant a memorial tree for Paris Kanellakis and his family

Design of On-Line Decision-Making Solutions for Time-Critical Planning and Scheduling Under Uncertainty." Lloyd will be a post-doctoral fellow in medical informatics at the University of Pennsylvania.

Brown CS has had its second Academy Award winner: Scott Anderson '86 got the "best visual effects" award for his work in *Babe*. Scott last appeared in these pages in Vol. 2 No. 2, in a discussion of Brown CS students in Hollywood, where we noted his work on *Terminator 2* and *The Abyss*. Scott seems to have good taste in movies: all of these are classics of their genre. Scott, who was also co-captain of the Brown wrestling team, was invited back to Brown this last year to give one of the graduation forums on his work. Unfortunately, he was scheduled opposite a talk by Marvin Minsky, legendary computer science/artificial intelligence guru and my thesis advisor, so I missed Scott's talk, but I gather it was great. (For a trivia question, who was the first Brown CS student to receive an Academy Award? Answer on the back page.) Eric Albert '80 is another grad in the entertainment business, so to speak. As noted in ***conduit!*** Vol. 3 No. 1, Eric makes his living by constructing crossword puzzles, which he does with a computer program of his own design. Recently *The New York Times* ran an article on computer-generated crossword puzzles along with a picture of Eric, feet up on his desk, mouse at the ready. Eric is described as "well known in the crossword industry for his elaborate proprietary software." The article also includes one of Eric's puzzles entitled "Artificial Intelligence," which rather pleased me since, if I remember correctly, Eric took my AI course in my first year at Brown. (Suzi Howe just checked: he did, and he got an A with distinction!)

There has been a rash of clever T-shirts sighted around the department. Some of my favorites are shown on the back page.

In the waning weeks of this summer, some signs appeared on various departmental bulletin boards (and in other places where people congregate, like next to the coffeemaker) that read "Kerri—I'm really sorry we fought like we did last night, I'd never do anything to hurt you. I was wrong—please forgive me—Ed". The signs, as you might imagine, generated a lot of discussion, from "Why can't this younger gen-

Conference in Philadelphia. In the summer he was invited for three weeks by the Academia Sinica of Taiwan to lecture and to participate in collaborative research at its main campus in Nankai, Taipei. In August he was pleased to receive one of the first copies of his *Lectures on Parallel Computation* published in Japanese by his colleagues at Kyoto University.

John Savage. In June John completed six years as a member of the board of directors of the Computing Research Association and chair of the Publications Committee. He is now vice-chair of Brown's ACUP, the Advisory Committee on University Planning, which is the student/faculty/administration committee responsible for analyzing the University's budget and making recommendations to the President. The Provost chairs ACUP. John also joined the Board of Managers of the Faculty Club as President-Elect. His book *Models of Computation: Exploring the Power of Computing* is nearing completion and he is using it to teach CS51, the first theory course required of all CS concentrators.

Roberto Tamassia. Roberto has joined the editorial board of *IEEE Transactions on Computers* and has been appointed chair of the steering committee of the graph drawing symposium. In June he chaired the Working Group on Computational Geometry at the Workshop

FROM THE CHAIRMAN, Eugene Charniak

Eugene Charniak

We are proud that our receptionist Dawn Nicholaus was one of thirteen recipients of the 1996 Brown Says Thank You awards for distinguished staff service. The competition was fierce this year, with over sixty people nominated. Dawn has been with the department since 1989, but has been associated with Brown for much longer. Indeed, she started her relationship with Brown by participating in a Brown-run outreach program in which ten students from local high-schools were identified and mentored in anticipation of future employment here. Those chosen were given part-time after-school jobs at Brown, but only two actually became full-time Brown employees—one works in the budget office and the other is our Dawn Nicholaus. Congratulations, Dawn!

Award winner Dawn Nicholaus

Just a few weeks ago we had a tree-planting ceremony to commemorate Paris Kanellakis, Maria-Teresa Otoya, and their two children. The tree is in Lincoln Field (the lower green) and is a Norway maple that should grow to become quite big. The ceremony was attended by about sixty of us, from CS and Psychological Services, where Maria-Teresa worked, and by other friends and neighbors. It was quite simple. Janet Cooper-Nelson, the University chaplain, said a few words, as did I, and then each participant in turn put small shovelfuls of earth on the roots of the tree, something we all found quite moving. We'll be putting in a memorial plaque later—we wanted to plant the tree early enough in the year that it could regenerate some roots before winter, and the plaque could not be ready in time. So instead we will have a second ceremony to install the plaque on December 20th, the first anniversary of their deaths.

Four graduate students have successfully defended their theses since the spring. **Darren Vengroff**, whose topic was "The Theory and Practice of I/O-Efficient Computation," is now teaching at the University of Delaware in the EE Department. **Hsueh-I Lu** is teaching at National Chung-Cheng University in Taiwan. His topic was "Efficient Approximation Algorithms for Some Semidefinite Programs." **Michael Littman**'s topic was "Algorithms for Sequential Decision Making." He is teaching at Duke University. **Lloyd Greenwald**'s was the most recent defense; his topic was "Analysis and

fac.activities@cs.brown.edu

Eugene Charniak. Ernest Davis (son of Brown Applied Math Professor Phil Davis), in a retrospective review of Hofstadter's *Godel, Escher, Bach: An Eternal Golden Braid*, attempted to give a feel for the *zeitgeist* when Hofstadter's book was published and how it differs from today's by contrasting two works by Eugene—his 1974 Ph.D. thesis and his recent book *Statistical Language Learning*. Says Davis, "The later book has many advantages over the earlier: the material presented is solidly grounded in statistical theory; it has been implemented and extensively tested; and the book is a model of clear writing. By contrast, the earlier book was unimplemented and often vague. The earlier Charniak did not know what he was doing, whereas the later Charniak knows what he is doing very precisely. But, on the other hand, the doctoral thesis dealt with a profound problem—the relation of knowledge and inference to natural language understanding—and pointed our understanding of this issue in a potentially revolutionary direction. I am still romantic enough to believe that, in the long run, Charniak's earlier work will be more influential."

Tom Dean. In August, Tom participated in several events at AAAI '96 in Portland, Oregon. He gave an invited talk jointly with Peter Bonasso of NASA's Johnson Space Center that concerned the history and future of the AAAI Robotics Competitions, the first of which they coordinated in 1992. He was also on a panel (chaired by Bart Selman from AT&T; the other panelists were Rodney Brooks, Eric Horvitz, Tom Mitchell and Nils Nilsson) in which each panelist issued a set of challenges for research in AI. Together with Leslie Kaelbling, Tom gave a tutorial on partially observable Markov decision processes and also ran a workshop on "Theory and Practice in Planning." At ECAI '96 in Budapest, he gave an invited talk at a workshop on planning. Afterwards he spent a week working and lecturing at DFKI (the German institute for AI) in Saarbrücken, Germany, and then went to Aalborg, Denmark, to serve on a thesis review panel as the primary 'interrogator.'

Maurice Herlihy. Maurice is currently involved in a variety of activities—chair of the steering committee for the ACM Symposium on Principles of Distributed Computing (PODC), a member of the ACM thesis award committee and editor for ACM *Transactions on Computer Systems*. He is on the advisory committee of Dartmouth's Master's Program and is editor of *SIAM Journal of Computation* and the *Chicago Journal of Theory.* He is co-chair of the 1997 Israeli Symposium on Theory of Computing and Systems.

Leslie Kaelbling. While on sabbatical, Leslie gave a tutorial on partially observable Markov decision processes (with Tom Dean) at AAAI; she was elected to the AAAI Executive Council. She served on a dissertation committee at the Université de Caen and lectured at CEMAGREF (a research lab in Paris) and the Université Libre de Bruxelles.

Robert Netzer. Rob has filed a patent application for instrumentation technology to support program debugging. It enables the programmer to surf through a program's execution history at will, going forward and backward through past states, optionally in response to queries about how data and control flowed through the execution. Several technological breakthroughs make this possible; programs run only about twice as slowly and traces are small enough to accommodate tracing a day-long run to a single gigabyte disk. Siemens Corporate Research is funding further development of some tools based on this technology; other industrial connections are on the horizon.

Franco Preparata. During the spring semester Franco presented Distinguished Lectures at Duke University, the University of Virginia, and Texas A&M University and in June he participated in a panel on robust computation at the Applied Computational Geometry

This work was largely motivated by spatial databases, an important new application area. While applications like these require conceptually infinite relations (e.g., to represent points in a rectangle), it is enough to store these relations using a finite representation such as constraints. Gaby completed his talk by describing results in complexity, expressibility, and indexing for constraint databases.

All of us in the audience felt that we had been treated to a wealth of technical topics that covered a wide variety of areas. We got a glimpse into the breadth and depth of Paris's technical contributions to computer science. We all miss him badly, but thank him for results he has left behind.

Before, during and after—over the summer we watched from the 4th floor deck as the former Math Department and Richardson dormitory were demolished to make way for the W. Duncan MacMillan '53 Hall, an undergraduate science teaching facility for chemistry, geology and environmental science

Symposium speakers from l to r: Gabriel Kuper, Harry Mairson, Moshe Vardi, Stan Zdonik, Alex Shvartsman, Pascal Van Hentenryck and Serge Abiteboul

THE 17TH IPP SYMPOSIUM

Co-hosts Stan Zdonik (above) and Pascal Van Hentenryck

On May 3, 1996, the Department hosted its 17th Industrial Partners Program technical symposium. This very special symposium celebrated the research career of our colleague and friend Paris Kanellakis, who was lost last December on American Airlines Flight 103 in Cali, Colombia. The speakers were all close associates of Paris's who had published at least one paper with him. Each of them gave a short overview on one of Paris's research interests and then described Paris's contributions to the area.

Serge Abiteboul from Stanford began by describing a formal model of object-oriented databases that he and Paris developed jointly in 1988-89, while Paris was on sabbatical at INRIA in France. The model introduced a query language IQL, based on Datalog, that makes object identity explicit and contains operators to manipulate objects, object identifiers (oids) and values. Basic IQL is not complete in that it is impossible to construct certain legal structures within the language. This problem is solved by introducing the curious operator *choose* that returns any oid from a set of oids. Serge argued that IQL forms the underpinnings for the emerging object-oriented database query language standard OQL.

The next speaker was Moshe Vardi from Rice University. Moshe spoke on Paris's work in global optimization for database logic programming. He described the notion of boundedness as an example of this style of optimization. A recursive logic program is bounded if it can be evaluated in a finite number of iterations; this is important since in this case, the recursion can be eliminated. He then described a theorem of Paris's that characterized when a program is bounded, and also described complexity results for these problems.

After lunch, Alex Shvartsman from MIT described some of his joint work with Paris in fault-tolerant parallel computing. The basic premise in this work is the inherent tension between efficiency and fault tolerance: efficient parallel algorithms demand a reduction in redundant computations, while fault-tolerant algorithms require more redundancy. Alex illustrated the design of algorithms that balance these two goals with a few interesting case studies, one of them an algorithm for the *write-all problem* that writes the value 1 into each array location of an *N*-element array using *P* processors.

Harry Mairson from Brandeis continued with a presentation on Paris's work on the complexity of programming languages. This work includes three fundamental results: a proof that first-order unification is complete for polynomial time, a proof that type inference for polymorphically typed functional programming languages is complete for exponential time, and several significant results on the expressibility of simply typed lambda calculus.

The final talk of the day was given by Gabriel Kuper from INRIA on the topic of constraint databases. This topic of current research interest was introduced by Paris (with Kuper and Peter Revesz, Ph.D. '91) in a 1990 paper.

remote town in Ethiopia to teach math. It did not take long to discover that that country had far more pressing needs, and after a stay of two months instead of the anticipated two years, he returned to the US only to find his draft number was 14! He then joined the Army Reserve and trained as a combat engineer and demolitions specialist at Fort Leonard Wood, MO. One of his projects involved building a helicopter firing range, which required clearing a vast area using a smorgasbord of explosives. It was decided, somewhat recklessly, that this project would be good for training new troops for demolition duty and 200 raw recruits learned on the job.

At home in the 5th floor machine room

The ensuing explosion accomplished its mission, but because of the inexperience of those laying the charges, many didn't detonate, leaving the area a highly perilous place to work—it also cracked the post commandant's fish tank! Another of his duties involved wiring charges to create realistic combat conditions for rifle squad training. On one occasion, a particularly gung-ho lieutenant brought in tons of charges and ordered live machine-gun fire for the squads as well as overhead—this made for some harrowing moments. Jeff's carefully calibrated system worked perfectly for two days until one unerring marksman hit a junction box (somewhat reminiscent of life at CS!).

Jeff is simply not given to gaffes, so amusing anecdotes are hard to come by. Tstaff call him 'Ice Man' and tease him for keeping his office at refrigeration temperatures—no one falls asleep in Jeff's staff meetings! His is also the neatest, most orderly office in the Department; papers are lined up to the edge of the desk and large expanses of desktop are visible. He has also been kidded about his love of power tools ("Home Depot Man"), for his meticulousness and for taking three years to reshingle his house despite having borrowed a pneumatic nailer to speed the process.

He prizes his Parker Duofold fountain pen and enjoys talking pens with Stan Zdonik and viewing Stan's significant collection. Jeff's macho persona is confirmed by Kathy Kirman, who came across him one day holding a bloody towel to his face—he had been whacked with a squash racquet and took much convincing to go the emergency room, where a plastic surgeon sewed up the gash with 10 stitches. Tstaff consider Jeff the perfect boss—he is fair and open-minded—however, they are given to delivering bad news *before* he goes jogging!

Jeff is a direct descendant of Roger Williams, founder of Rhode Island, who emigrated from England in 1630; the Briggs line of his family traces as far back as the twelfth century to Ynir, King of Gwentland (Wales). One of the more alluring ancestral names is Freelove Bliss, 1692, of Westerly, RI. The Bates line was researched by Jeff's great-grandmother, who received her MA at Brown in 1883 and was for a period Alumni Registrar. Her genealogical study comprises 85 handwritten volumes and is housed in the RI Historical Society. Jeff and his siblings have middle names associated both with their heritage and, interestingly, with streets within blocks of this building—Waterman (jwc), Angell, Williams and Bowen. He enjoys nature photography and landscaping and is also a fitness buff who can be found in the Athletic Center weight room at noon when he isn't running around the East Side. His family includes his wife, Donna, a golden retriever (Donna's shadow ever since she pulled him through a life-threatening illness), a cat (the ferocious hunting kind) and a lovebird. His son, Jason, is a student at UMD, his daughter, Kristen, at UNH—neither is interested in the sciences.

read. This may be nothing more than a natural competitive process and one that will work itself out eventually. After all, unlimited growth in any area cannot continue indefinitely without depleting the available resources. Electronic publishing will change the cost structure of research publication and give authors and the reading public more opportunities. It is an exercise that needs to be played out.

A side effect of the high cost of publication is that many publishers are insisting that the copyright laws be strictly enforced. Multi-million-dollar awards have been made to publishers by the courts. As a consequence, some universities have become extraordinarily sensitive to this issue. Our university is warning faculty members that they will be subject to sanctions if they do not follow the law exactly. When the law is explained, many of us find it not only ambiguous but also very distracting. The good news is that ACM has changed its policy recently to allow classroom use of their copyrighted material. This enlightened policy should be emulated by other publishers, a position taken by the CRA Board at its December meeting, because it serves them and our research community. Their copyright statements will be visible to student readers, drawing them to the publishers, while the research material, which is supposed to serve the community, becomes more readily accessible.

JEFF ‘Ice Man’ COADY

For more than 13 years now, CS faculty and students who visit other departments of computer science have returned full of praise and appreciation for the functionality and reliability of the Department’s computer systems. This well deserved praise is due in large part to the efforts of Jeff Coady, our director of computer facilities and manager of the eight-person technical staff. Since his arrival in ’83, Jeff has been at the technical core of the Department, responsible for integrating faculty research interests and equipment requirements with the more generic needs of the Department—a challenging task requiring know-how, diplomacy and vision.

Dave Durfee, hired by Andy van Dam to install the newly acquired Apollo systems, made the initial contact with Jeff, who was subsequently hired as system administrator. At that point the technical staff consisted of Jeff, Dave, John Bazik, Max Salvas and three former graduate students—Joe Pato, Dave Johnson and Marc Brown. Jeff describes his first seven years as ‘absolute hell,’ breaking new ground initially with the largest Apollo network in the world (including at Apollo). It took several years to refine our network management to the point that the network functioned satisfactorily despite its lack of computing power. In ’88 the Department moved into the new CIT building and new equipment was in order. Sun3s replaced the Apollos and were replaced a year later by SPARCstation1s. A 1992 upgrade decision culminated a two-year process that entailed significant faculty-tstaff cooperation. Of the five major vendors involved, the finalists were Sun and IBM, with Sun SPARC10s the ultimate choice. The original black and white Apollos were .5 MIPS with one meg of memory and relied on the network exclusively, in contrast to the current color SPARC10s which perform at 110 MIPS and have 32 Mb of memory and either a half- or one-gig local disk.

> *“The original black and white Apollos were .5 MIPS with one meg of memory and relied on the network exclusively”*

Acquiring new equipment is always a challenge. Within a year or so, the Department will again replace its current machines—Jeff and the chairman are already involved in negotiations. The network, consisting of 175 machines and servers that support up to 1,000 users each semester, is currently undergoing a major upgrade. Work has been in progress to upgrade the Ethernet from 10Mb to 100Mb, and at the same time fiber-optic cable is being pulled to provide for future upgrades.

Before joining CS, Jeff worked at Motorola-Codex for two years and then put in a stint at Raytheon. He had joined the Peace Corps directly after college and was shipped to a

RESEARCH PUBLICATION MODES RECONSIDERED

Franco Preparata

John Savage

The rapidly developing public interest in the World-Wide Web is causing many in the research community to propose that the Web become an integral part of the publication process. Although technological breakthroughs often profoundly alter established modes of operation, it is important to choose carefully the options they offer without sacrificing the good features of the old modes.

DISCLOSURE VS. PUBLICATION

In the dissemination of research results we should distinguish between two major objectives: disclosure and publication.

Disclosure is used to make results immediately available to a research community. Traditionally this function has been served by author-published research reports and, to some extent, by conference proceedings for which the publication delay is within reasonable limits. For this function the World-Wide Web is ideally suited. However, for it to be a success, the number of Web sites holding professional materials should be limited and/or good Web search engines need to be employed.

Anyone who has spent more than a few minutes using one of the general Web search engines is aware of the enormous amount of highly superfluous material that can be generated. On the other hand, experience with area-specific database search programs, such as Glimpse, demonstrates they can be enormously useful. That's both good and bad news because it's very easy for papers that are not indexed in a well-known database to get lost like the proverbial needle in the haystack.

Unfortunately, the disclosure process described above does not provide the close scrutiny that is provided by the journal reviewing process. On the other hand, journal publication in computer science is typically handicapped by a very long reviewing process. Fortunately, the outrageous publication delays we experience today are not intrinsic to journal publication. In other fields, notably physics and biology, journal reviewing is done in a matter of months. Not in computer science; papers languish for years. Given the long delays in journal publishing, it is no wonder that it is not encouraged by some senior members in our field.

REVIEWING PRACTICES

Conferences by the very nature of their reviewing process cannot provide the rigorous standards that are enforced by the best journals. Conferences, however (even the most prestigious and highly competitive ones), have popularized a style that sometimes at best falls short of standards and at worst hampers future research. Limited space has licensed withdrawal of details (proofs omitted): unfortunately, this has become the practice even when the length of the paper is well below the allowed maximum. When a conference paper in this format is not expanded for journal publication, a potentially fruitful area of research is stifled.

> *"Electronic disclosure is necessarily generating clutter but timeliness may fully justify this. It is the function of publication to redress this shortcoming"*

Electronic disclosure is necessarily generating clutter but timeliness may fully justify this. It is the function of publication to redress this shortcoming by letting a vast peer community pass judgment on disclosed research. The World-Wide Web could supplement traditional media in facilitating access. However, it could be very dangerous to replace the traditional editor/referee pool with individuals fully in charge of selectivity. This would remove the feature of anonymity which is crucial to the maintenance of high standards.

OWNERSHIP OF COPYRIGHTS

The cost of journals continues to grow at an alarming rate. As a result, research libraries are dropping less popular journals to make room in their budgets for more popular ones. Journals are increasing their charges because their costs are growing. In the process authors are losing opportunities to have their work

MICHAEL LITTMAN Ph.D. ’96

How’s life in Providence? There’s lots of things I miss about Brown, but I do prefer life as a faculty member to life as a grad student! The staff here is putting together a newsletter and they want me to write a short blurb for a ‘new faculty spotlight.’ For guidance, I figured I’d take a look at back issues of ***conduit!*** on the Web. It’s clear that there’s no way I’ll be able to achieve such a high standard of journalistic excellence! :)

mlittman@cs.duke.edu

RANDY PAUSCH ’82

Randy got his Ph.D. at CMU in ’88 and since then has taught at the University of Virginia, where he has become an NSF Presidential Young Investigator and a Lilly Foundation Teaching Fellow. Most recently, he spent a sabbatical with the Walt Disney Imagineering Virtual Reality Lab working on the Aladdin VR project. In July, Randy gave a fascinating and lively lecture in the Department on the topic “Disney’s Aladdin: Steps Towards Storytelling in Virtual Reality.” His User Interface Group (blatantly patterned after Brown’s Graphics Group) has recently developed a free, easy-to-learn 3D graphics package in the spirit of “LOGO meets VisualBasic”—it’s called Alice and can be downloaded from *alice.virginia.edu*.

pausch@virginia.edu

JOHN STASKO Ph.D. ’89

1995 was a busy year for me. In the spring I received tenure at Georgia Tech. So I’m now an Associate Professor in the College of Computing. Our unit with about 40 faculty is a big change from the small department model I was used to at Brown. Here at GT I’m a member of the Graphics, Visualization, and Usability (GVU) Center too. It’s an interdisciplinary campus unit made up of faculty who do research in those areas. Last fall I also began a two-year stint as Graduate Coordinator. That has consumed a great deal of my time. Even bigger news is that last fall I got married! My wife, Christine (Rich), is a project manager for Medaphis Corporation here in Atlanta. Kevin Brophy, my old grad school roommate and best friend, was able to come down from Brockton, MA, to be my best man. Right before we got married, Christy and I bought a new home up in Marietta, a suburb just a little northwest of Atlanta.

I still try to play as much golf as I can, though often it’s not enough :^), and I’ve become a big Atlanta Braves fan. This summer Christy and I enjoyed going to a number of different Olympic events. If any old-timers are ever in the Atlanta area, please drop by and say hello. My URL is *http://www.cc.gatech.edu/gvu/people/faculty/john.stasko*.

stasko@cc.gatech.edu

CHICKEN-SEXING—the last word (honest)

IRVING BIEDERMAN

Thank you so much for sending the Spring 1996 issue of ***conduit!*** to me. My condolences to you and your colleagues on the tragic loss of Dr. Kanellakis and his family. I was most touched by the memorial to him.

I loved your account of our chicken sexing exchange. Of course it was deeply gratifying to read our work described as a “landmark paper.”

But let me compliment you on ***conduit!*** It is beautifully written, has real content rather than pap, takes some risks, and is so handsomely produced that I am sure you are the envy of in-house publication staffs from MUCH larger institutions.

William M. Keck Professor of Cognitive Neuroscience, Dept. of Psychology, USC.

USCbieder@mizar.usc.edu

ROBERT STERN

Thanks so much for thinking of sending me the copy of ***conduit!*** I and my colleagues here were very tickled to receive it and I really appreciate your being so considerate.

Thanks to your leads, I can now consider myself something of a chick-sexing expert, but alas it seems that the Asian angle I was originally pursuing was a false one—what I had thought was a uniquely Korean skill turns out to be taught at two chick-sexing institutions in the States alone! Oh well, you win some, you lose some, as the day-old chicks say to each other.....

Reporter, CNBC, Asia (Hong Kong)

Corp. We specialize in enterprise management solutions (you know, network management, SNMP, OpenView, etc). We currently have teams working with about a dozen clients in the Boston/Washington corridor, mostly in the NY/NJ area.

With a little luck I'll be celebrating my 22nd wedding anniversary in January, and will be sending children off to college in 1999, 2002, and 2007.

acohen@unified.com

DILIP D'SOUZA M.Sc. '88

I think I lost something of myself when I read about Paris Kanellakis and his family in the *Brown Alumni Monthly* and then ***conduit!*** recently. Paris was a good friend while I was at CS getting my MS. He may not have known it, but his always ready smile and helpful words for me—in his office or even in the corridors of Kassar House—helped this raw, nervous and far too wide-eyed young Indian student find his feet at Brown and in the USA. Later, when I was searching for my first ever job, he wrote me a warm recommendation letter. I'm not sure I fully deserved what he said about me in it, but that was how I knew Paris—gently encouraging at the very times I didn't believe in myself. You meant a lot to me then, Paris. How sorry I am that I didn't tell you that enough.

What am I doing now? In a phrase: very little CS any more. I'm metamorphosing into a journalist. Since I returned to India in early '92, I've been writing for the press here on the side, as a hobby. I soon found out two things: that I was doing more and more of the writing, and that I was enjoying it much more than in CS. Now my writing income by itself is enough to keep us (my wife and I—I'm coming to that) clothed and fed and whatever else incomes do. I'm still with SPA Software on a kind of consulting basis, mostly looking after a small team of guys who do some AutoCAD work for a company in Portland, OR.

I have at least three columns a week: two are kind of political/current affairs commentary, and the third is a science column that's syndicated. Besides, I've just agreed to do a fortnightly column (again, politics/current affairs) for a Web site based here in Bombay, and I try to do at least one other longish piece a month for some paper or the other. I also have done a lot of travel writing on some interesting places I've been to (Cuba most recently, Argentina, Madagascar, etc.). I'm constantly running into people who have read something I've written, which is nice to know. Another good sign that I'm being read is that I get a fair amount of hate mail!

I married Vibha Kamat in December 1993. She teaches French here at the Alliance Française.

Moving back to India was the best thing I ever did in my life, you know. Discovering a passion for writing is one reason. Vibha is the other.

vibha@dilip.ilbom.ernet.in

***Axsys** technician sorting cables in one of two network closets*

Pulling cable—4 twisted-pair and 2 fiberoptic

Terminating a distribution panel prior to final testing

See page 9 towards the bottom of the page for more on the Ethernet upgrade/cabling

It was thus decided that a major goal of WICS in 96/97 would be to foster a supportive social environment for women in the department, beginning during the week of First-Year Orientation at Activities Night. Valerie Green and Elena Jakubiak spent two hours taking down names for the WICS mailing list, discussing course options with first-year women and dispelling many of the misconceptions associated with the Computer Science Department. It was astonishing to hear what some academic advisors from other departments had to say to their female advisees who were interested in computer science—one first-year said her advisor had told her that if she took CS15, she would be spending 40 hours a week on it, would have no social life, and would have little or no time for her other courses. After hearing other reports from first-years of similar remarks received from counselors, advisors or other students, it seemed fortunate that the first-years who came to the WICS table at Activities Night were able to hear a second opinion!

With increased support for new female students in the department, WICS hopes to attract and retain more women in computer science than in past years. The first WICS meeting of the semester attracted 21 participants, a large increase from the six or eight members of previous years. WICS will continue to sponsor events for women in the department and will be participating in other gender-related discussions and activities coordinated by GIICS, a group for men and women interested in gender issues in computer science.

EMAIL TO THE EDITOR *et al*

PAUL ANAGNOSTOPOULOS '79

John, Rather a while since I've been in touch. As you may know, I went to MIT grad school, but only lasted one semester. Too much school, I guess. Worked at various companies: Wang, two start-ups, Digital, etc. until 1988. Left Digital to work for myself, which I've been doing since. Slowly retired from the software business, which has gotten too insane for me (requires 25-year-old's energy and excitement). Now I make most of my money designing and typesetting books, largely of the technical variety. I do a software gig every now and again when the madness level is low enough. Hope everything is well in the department. We really should have a Brown CS reunion sometime. I can wear my badge "First Brown C.S. Graduate." Take care.

greek@windfall.com

ROBERT (BOBBY) BLUMOFE '88

Andy, for what it's worth, I see that Brown was number two in "graphics: user interaction" in the *US News & World Report* survey. Of course, they might be off by one, but in any case, I believe I know why Brown is so highly regarded in this area. Congratulations!

By the way, I want to express my sorrow and offer my condolences with regard to Paris. He served as undergraduate advisor when I was an undergraduate; he was always sympathetic and always helpful. I'm thankful that I had the opportunity to visit Brown last year and speak with Paris as a colleague.

An update for ***conduit!***—I received my bachelor's degree from Brown University in 1988 and a Ph.D. from MIT in 1995. My research career in computer graphics began at Brown with Andy. I did my Ph.D. work on algorithms and systems for parallel multithreaded computing with Charles Leiserson at MIT, for which I received the George M. Sprowls Doctoral Dissertation Award from the MIT Department of Electrical Engineering and Computer Science. As part of this dissertation work, I developed an algorithmic theory of multithreaded computation and designed and implemented a multithreaded language and runtime system, called Cilk, that is based on the algorithmic theory. In addition, I developed an adaptive and fault-tolerant version of Cilk, called Cilk-NOW, that runs on networks of workstations. I'm now an Assistant Professor at the University of Texas at Austin, where I'm continuing my work on Cilk and Cilk-NOW.

rdb@cs.utexas.edu

AARON COHEN Sc.M. '76

conduit! readers: I enjoy reading about what each of you is doing, especially those of you from ancient times when I attended Brown.

An update on me: I am no longer with Bell Labs or AT&T. For the last four years I have been with Unified Systems Solutions, which is now a subsidiary of Computer Horizons we set up the environment to model some situation or protocol, and the students are faced with some challenge, e.g. decrypting a message or taking advantage of a security flaw in the protocol.

With the help of funding from the National Science Foundation, I plan to develop the course materials and software to the point that I can disseminate them via the Web to others who might teach a similar course. As digital security becomes ever more a part of daily life, and as we as citizens confront controversies such as export controls on products that incorporate cryptography, it becomes more important to spread awareness of the principles of digital security—and of the contributions of computer science and mathematics to this field.

50/50 by 2010

Valerie Green, WICS coordinator

"50/50 by 2010." This is the goal of Dr. Anita Borg, founder of the Systers Academia organization for women in computer science on the Internet. By the year 2010, she believes that half the graduating engineers and scientists can be women. Currently, many businesses, colleges and universities are working to increase under-represented groups in many scientific fields, and Brown is no exception.

After the subject of female representation was aired in the course of a National Science Foundation site visit last spring, the Brown undergraduate group Women in Computer Science gathered to discuss methods of attracting women to the field of computer science. Many women in WICS had come to the department during their sophomore year, often after hearing about computer involvement in other fields that interested them, such as art, music, film, animation, math and economics. Many of these women talked about overcoming the 'computer geek' image and about withstanding warnings from friends regarding the workload. Looking back, most felt that descriptions of the computer science curriculum by non-majors were not generally accurate. And several women wished they had been exposed earlier to computer science at Brown, since the field had not been stressed during their secondary education and consequently was not an area they had previously considered exploring.

With these comments in mind, WICS decided to recruit women to the computer science department by providing information and positive descriptions of the curriculum and the department in general. WICS put some of a generous donation received last spring from Motorola toward this outreach project. Tashana Landray and Michael Radwin designed a postcard, to be sent to all females accepted to the class of 2000, featuring a picture of Ada Lovelace (below) and stressing computer science and its ties to many different areas of study. To encourage questions from prospective first-year students, each postcard also included the name, email address and telephone number of an undergraduate woman in the Computer Science Department. This personal interaction also allowed WICS members to portray the Computer Science Department in a more favorable light than is sometimes provided by first-year advisors, counselors, and other students. 1600 postcards were sent, and many members of WICS were delighted to receive telephone calls and email from interested women who wanted to know more about what computer science at Brown had to offer.

After the initial mailing, two questions in the minds of WICS members were, 'Will the postcards work?' and 'How do we keep women in the department after they enroll in CS15?' (In past years, the dropout rate of women in CS15 has been much higher than that of men.) WICS members ultimately concluded that a major reason for the higher dropout rate was the feeling of isolation common among many women in computer science, a well documented problem discussed frequently in newsgroups and mailing lists for women in the computer industry.

who knows the secret key can construct a valid signature for a given document, so a valid signature associated with a document is strong evidence that the creator of the keys was responsible for producing the signature. If someone tampers with the document, the signature will no longer bear the same mathematical relation to the document, so the document will be deemed invalid. Digital signatures can thus be used to authenticate messages sent over the Internet, guarding against undetected tampering and forged messages. They can be used for creating unforgeable certificates, such as an electronic version of a credit card or passport. They can also be used to detect unauthorized changes to a computer program, such as the introduction of a virus.

The MarkCalc—Eve attempts to intercept Alice's message to Bob

Other technologies for computer security have been developed, including methods for securely authenticating a party (the secure analogue of reciting a phone card number or credit card number over the telephone), methods for committing to a document without revealing it (the secure analogue of a sealed envelope), and methods for time-stamping a document (the secure analogue of mailing oneself a letter in order to get it postmarked).

The technology of cryptography rests on the science of computation in that it crucially relies on the fundamental premise of that science, the dichotomy between computationally easy problems and computationally difficult problems: codes must be easy to decrypt if you know the key, hard if you don't. Cryptography is thus a concrete realization of this intellectual pursuit.

In order to expose a broader audience to the excitement of a fun, increasingly important, and intellectually challenging field, I have started a course called "Secrets and Promises: Digital Security and Its Implications." The course is open to all students but is aimed at those with no prior background in computers or programming. Peter Galea '96 (now at Tera Systems, Inc.) and Sarah Finney '97 have helped me organize the sequence of lectures. I teach a little of the mathematical background, including some number theory, probability theory, and the growth rate of functions. The mathematics is used as a tool to better understand what security means. The students learn about the various security technologies discussed above and how they can be combined in applications such as electronic cash.

This is not a course in the practical aspects of using commercial security software, nor does it turn out instant experts in security; my goal is to impart to students a conceptual understanding of digital security as an application of fundamental ideas in mathematics and computer science. Students learn firsthand some of the security flaws that can arise in carelessly designed systems. They 'program' cryptographic protocols such as might arise in applications like electronic payment schemes, voting, and lotteries.

The course is centered around a specially designed programming environment we call the MarkCalc. I designed the MarkCalc in collaboration with Mark Weaver, a former Brown undergraduate (now at Pretty Good Privacy, Inc.), and Mark implemented it. (It was given its current name over Mark's protestations.) One creates a calculator to represent each party in a protocol and 'programs' it to interact with the other parties. Arrows indicate communication between the calculators. One can model an eavesdropper intercepting or disrupting a communication. A typical assignment consists of a series of 'experiments.' For each experiment, tions from industrial espionage. Perhaps the most exciting applications, however, involve securing communication between parties that have no previous connection and have therefore had no opportunity to agree on a key in advance. As commerce on the Internet grows, such applications will become ever more prevalent. Fortunately, technologies such as exponential key exchange and public-key cryptography exist to make such applications possible.

Public-key cryptography, proposed by Diffie and Hellman in 1976, is the idea of having two separate keys, a public key for encryption of a message and a secret key for its decryption; a party can privately construct the two keys and then make the encryption key public without thereby revealing the decryption key. Subsequently, anyone can encrypt messages intended for the creator of the keys, but only the creator can decrypt. The first realization of this idea was due to Rivest, Shamir, and Adleman in 1978. The extent to which their scheme has captured the popular imagination is reflected by the following excerpt from a Harlequin romance, *Sunward Journey:*

> "I'm really not into computers, Jay. I don't know much. I do know the key to the code was the product of two long prime numbers, each about a hundred digits, right?"
>
> "Yes, that's correct. It's called the RSA cryptosystem."
>
> "Right, for Rivest, Shamir, and Adleman from MIT. That much I know. I also understand that even using a sophisticated computer to decipher the code it would take forever," she recalled. "Something like three point eight billion years for a two-hundred-digit key, right?"
>
> "That's exactly correct. All of the stolen information was apparently tapped from the phone lines running from the company offices to your house. Supposedly no one except Mike had the decoding key, and no one could figure it out unless he passed it along, but there has to be a bug in that logic somewhere," he said, loosening his dark green silk tie. "Vee, it's much warmer than I thought. Would you mind if I removed my jacket?"
>
> "Of course not. You're so formal," she remarked.....

As our heroine, Vee, states, RSA is based on properties of the product of two prime numbers. Thus it harnesses Hardy's favorite area of 'pure' mathematics, number theory. The basis of this cryptosystem (like most) is the dichotomy between easy and hard. Creating the public and secret keys is roughly as easy as selecting and multiplying the two hundred-digit prime numbers. As Vee asserts, cracking the system (using currently known methods) requires an exorbitant amount of time; it seems to require one to determine the two prime numbers from their product, a problem called integer factorization. Though progress on this problem continues, known algorithms for it are not fast enough seriously to threaten the security of RSA—not yet, anyway. To quote a man known more for marketing skill than expertise in number theory,

> Because both the system's privacy and the security of digital money depend on encryption, a breakthrough in mathematics or computer science that defeats the cryptographic system could be a disaster. The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers. (Bill Gates, *The Road Ahead*, p. 265).

(To factor a number is to determine the prime numbers which when multiplied together form the number; thus it is trivial to factor a number that is itself prime.)

"If someone tampers with the document, the signature will no longer bear the same mathematical relation to the document, so the document will be deemed invalid"

But RSA has uses other than encryption. As Diffie and Hellman realized, the flip side of public-key cryptography is digital signatures. Using a method such as RSA, the creator of the two keys can construct a *signature* for a document, a number derived from the document in such a way that anyone who knows the public key can verify the signature is consistent with that document. Furthermore, only someone

conduit!

Volume 5, Number 2 — Department of Computer Science — Fall, 1996
Brown University

CS 007: SECRETS AND PROMISES

Philip Klein

In his autobiography, *A Mathematician's Apology*, the number theorist and pacifist G. H. Hardy wrote

> ...both Gauss and lesser mathematicians may be justified in rejoicing that there is one science [number theory] at any rate...whose very remoteness from ordinary human activities should keep it gentle and clean.

Hardy's book was published in 1940, towards the end of his career. If he had postponed his judgment for another thirty years, he might have come to a different conclusion, for number theory became the basis for an important technology long associated with war: cryptography, the use of secret codes.

Cryptography has been in use for at least several thousand years. It is listed in the Kama Sutra as one of the 64 arts to be mastered by women (perhaps in anticipation of marriage). One cryptosystem is attributed to Julius Caesar (inexplicably, no historian has ever suggested that the weakness of his cryptosystem contributed to his downfall). Numerous anecdotes attest to the importance of cryptography in war and diplomacy over the years—and to that of cryptanalysis, the cracking of codes. For example, Britain's interception and deciphering of the Zimmermann telegram, a message from Germany's foreign secretary to the government of Mexico (via the ambassador), helped speed the United States' entry into World War I, for the message promised Texas, New Mexico, and Arizona to Mexico in return for its help against the US. Cryptanalysis has also played a role in somewhat less momentous events as well; the following is excerpted from the autobiography of Casanova (1757):

> Five or six weeks later, she asked me if I had deciphered the manuscript.... I told her that I had.
>
> "Without the key, sir, excuse me if I believe the thing impossible."
>
> "Do you wish me to name your key, madame?''
>
> "If you please."
>
> I then told her the key-word which belonged to no language, and I saw her surprise. She told me that it was impossible, for she believed herself the only possessor of that word which she kept in her memory and which she had never written down. I could have told her the truth—that the same calculation which had served me for deciphering the manuscript had enabled me to learn the word—but on a caprice it struck me to tell her that a genie had revealed it to me. This false disclosure fettered Madame d'Urfe to me. That day I became the master of her soul, and I abused my power.

"Do you wish me to name your key, madame?"......"That day I became the master of her soul, and I abused my power"

In the Information Age, however, cryptography's greatest contribution may be to commerce. Banks have long used cryptography to protect the security of electronic transfers. Geographically distributed corporations have used cryptography to protect their communica-