department NEWS

Faculty NEWS

Markus Banagl accepted a professorship at the University of Heidelberg in Germany.

Wlodek Bryc hosted several Polish mathematicians last year under his US-East/Central Europe Collaborative Research grant from the National Science Foundation. Last June in Bedlewo, Poland, he participated in a conference on Noncommutative Probability and Related Topics.

Jim Deddens spent September and October 2003 and March 2004 at IRAS (Institute for Risk Assessment Sciences) at the University of Utrecht in the Netherlands. While there he gave a short course on mixed models and presented colloquium talks at the University of Utrecht, Erasmus University in Rotterdam and the University of Nijmege. He also served on a PhD committee and was appointed to another, which will take him back to Utrecht this fall. In June he presented a paper at an exposure assessment conference in Utrecht, and in July 2004 he spoke at a conference on ergonomics in Zurich, Switzerland. Jim was also appointed to a Harvard PhD committee to work with an industrial hygiene student on her statistical analysis involving mixed models.

Jintai Ding gave presentations at the International Workshop on Public Key Cryptology. Together with Dieter Schmidt, formerly of this department but now in computer science, Jintai broke SFlash-v3, one of the new European security standards for smart cards.

Scott Dumas presented talks in Belgium and Germany last summer and at the Workshop on Relativistic Channeling and Related Coherent Effects in Frascati, Italy, last spring.

Chuck Groetsch was local organizer of the Mathematical Association of America Ohio Section spring meeting in Cincinnati this past March and also organized the SUSTAIN/EXCEL Meeting on Professional Development of Teachers at Wright State University. He is a co-investigator on a Transition to Teaching grant from the National Science Foundation. He, David Minda, and Joy Moore are co-investigators on a National Science Foundation Math/Science Partnership grant involving the Cincinnati Public School District.

David Herron lectured at the "Analysis on Metric Spaces" meeting this summer at the Stefan Banach International Mathematical Center in Poland. He edited *Future Trends in Geometric Function Theory*, proceedings of last summer's workshop of the same name.

Tim Hodges gave an invited talk at the International Conference on Quantum Groups at the Technion in Haifa, Israel this summer.

Paul Horn and Amadeo Pesce, of UC's medical school, are working on a book, *Reference Intervals: A User's Guide*. They taught a summer short course on reference intervals for the American Association of Clinical Chemistry. Paul is co-investigator or statistician on several grants from agencies including the National Institutes of Health and the National Institute of Occupational Safety and Health.

Sung Kim taught a short course, Quality Assurance for Air Pollution Measurement Systems, for the Environmental Protection Agency in Florida this August.

Tony Leung chaired a special session on partial differential equations at the annual meeting of the American Mathematical Society meeting last January. Tony is collaborating with G. S. Chen of the Engineering College in National Tsing-Hua University (Taiwan) on a partial differential equations model for plasma display technology.

Chris McCord spoke at a workshop on celestial dynamics at the Banff International Research Station last April. He was appointed an associate dean of the McMicken College, effective September 1, 2004.

Pat McSwiggen organized a special session on dynamical systems at the American Mathematical Society regional meeting in Athens, Ohio.

David Minda gave the plenary talk, "Some Geometric Gems Via Möbius Transformations" at the fall 2003 meeting of the Ohio Section of the Mathematical Association of America meeting in Ada, Ohio.

Joy Moore and **Steve Pelikan** were reappointed as Ohio Board of Regents Teaching Fellows.

Diego Murio organized the 2004 Inverse Problems in Engineering Symposium, held in Cincinnati last June.

Jim Osterburg presented a paper at the 15th Annual Latin America Conference in July 2003 in Cocoyoc, Mexico. Last June he spoke at a meeting in Halifax, Nova Scotia.

Costel Peligrad spoke at the Memorial Conference for Ioana Cioranescu at the University of Puerto Rico last August. This June he was invited speaker in a plenary session at the Twentieth Conference in Operator Theory in Timisoara, Romania.

Magda Peligrad was awarded a two-year grant from the National Security Agency to investigate dependence models in probability.

Steve Pelikan is working with Applied Conservation International and the Cincinnati Zoo on estimating populations of sea birds.

Nages Shanmugalingam was awarded a new three-year National Science Foundation grant to support her research. This summer she participated in "Analysis on Metric Spaces" at the Stefan Banach International Mathematical Center in Poland and the International Workshop on Potential Theory in Matsue, Japan. She also visited the Helsinki Institute of Technology.

Siva Sivaganesan made a presentation at the Workshop on Objective Bayesian Analysis in Modane, France last June. He has a research grant from the National Institutes of Health.

Tara Smith spoke at the Banff Workshop on Quadratic Forms last October. She was one of the presenters at the "Forward to Professorship" panel for pre-tenure women in science, engineering, and math at Gallaudet University in May.

Srdjan Stojanovic spent the spring quarter at the Institute for Mathematics and Its Applications in Minneanpolis. He gave several lectures there, including a short course, "Options Pricing, Portfolio Hedging, and Data Analysis." He also presented a talk at an international meeting on Monte Carlo methods at Juan-les-Pins, France, in June 2004. Last year he ran a mock stock market for the Fairview Elementary School Math Night.

Gary Weiss is faculty adviser to UC Skeptics, a student club.

Bingyu Zhang made presentations last summer at the University of Strasbourg and Institut Elie Cartan (Université de Nancy 1) in France.

Student NEWS

Undergraduate Student News:
The department graduated 14 seniors this year. Undergraduate award winners for 2003-2004 included Carl McTague (Jeanne Gulden Scholarship), Gregory Hull (Harris Hancock Undergraduate Scholarship), Sabrina Blakeman (Feld Scholarship), Allen Miller (Buck Scholarship, A&S Mathematics Scholarship), Afshan Adhami, Jess D'Souza, Nicholas Graham, and Jon Slovisky (Harry S. Kieval Scholarship), Ben Cerniglia and Jon Slovisky (Linder Book Award).

Congratulations to Sabrina Blakeman on her recent marriage to PhD student Chris Camfield.

Graduate Student News:
The department graduated 30 MS students and two PhDs, Guojun Wang and Weiming Yu. Ying Shi and Zhijun Yin won Taft Advanced Graduate Fellowship Awards for 2004-05. Raluca Dumitru won the Neff Fellowship Award to allow her to accompany her adviser, Costel Peligrad, to Italy during his sabbatical. Anahit Galstyan won the Henry Laws Fellowship Award as well as the department's Outstanding Graduate Assistant Award. Christopher Camfield received the Outstanding Beginning Doctoral Student Award. Annette (Christianson) Ellis was given the department's Outstanding Masters Student Award.

Alumni NEWS

DENNIS BERKEY (PhD 1974)
The Board of Trustees of Worcester Polytechnic Institute (WPI) has elected Dennis D. Berkey as the university's 15th president. He was among more than 130 candidates nominated for the position. A native of Ohio, Berkey earned a BA in mathematics from Muskingum College in New Concord, Ohio, and an MA in mathematics from Miami University in Oxford, Ohio. Working under Al Lazer, he earned his PhD in mathematics from UC.

Dr. Berkey previously served as provost at Boston University, where he held the position on two different occasions totaling more than 13 years. In his role as chief academic officer for the nation's fourth-largest private university, he oversaw 14 BU schools and colleges, 29,000 students, the BU Corporate Education Center, and programs such as information technology, student life, international programs, and sponsored research, which totals $275 million annually. He also founded the Center for Teaching Excellence and the Undergraduate Research Opportunities Office.

As the dean of Arts and Sciences at BU from 1987 to 2002, Berkey headed 23 academic departments and 15 research centers. He introduced three new departments, computer science, cognitive and neural systems, and international relations, and developed a freshman writing seminars program and a college honors program. During his more than 20 years as an administrator, he also held positions of vice provost, associate vice president for academic affairs, and chairman of the department of mathematics.

Berkey is a member of the American Mathematical Society, the Mathematical Association of America, the Society for Industrial and Applied Mathematics, and the American Association of Higher Education. He has authored more than 15 peer-reviewed scientific papers and two calculus text books. In addition, he received the Metcalf Cup and Prize for Excellence in Teaching from Boston University.

Berkey resides in Weston, Mass., with his wife, Catherine, an accomplished member of academia in her own right. She is a lecturer at the Harvard Medical School and a research associate in medicine at Brigham and Women's Hospital. She holds a BA in mathematics with a minor in biology from Miami University, an MA in mathematics and statistics from Boston University, and a PhD in biostatistics from Harvard University. The Berkeys have three children.

MICHAEL CARR (BA 1980)
Michael Carr, Esq., CISSP has accepted the University of Nebraska's offer to be Chief Information Security Officer with oversight responsibility for the four state universities—the University of Nebraska at Lincoln, the University of Nebraska at Omaha, the University of Nebraska at Kearny and the University of Nebraska Medical Center. Mike was the Director of Information Services for Hamilton County Juvenile Court from 1994-2000 and has been working as an independent I/T security consultant and secretary of the Cincinnati Network Professional Association (CiNPA) for the past couple of years. A 1980 graduate of McMicken College, Mike also has an MBA from UC's CBA ('91), an MS in computer science from the University of Dayton('85) and a JD from the Salmon P. Chase College of Law ('01).

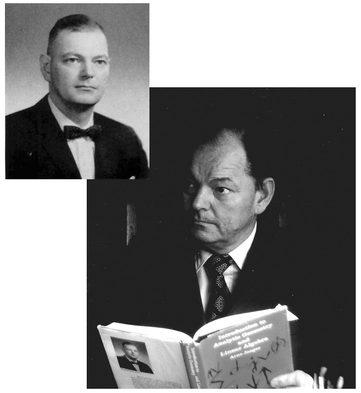
KATHLEEN (JAMES) NEIHEISEL (BA 1983)
Kathy writes, "Ten years ago I put on my coaching hat again. Not soccer, but for the national program Math Counts. This middle school program encourages and enriches budding mathematicians." Kathy currently coaches for Van Buren Middle School in Kettering, Ohio.

Please use the included form to include your latest news in the next issue of *the Right Angle* and other McMicken College publications.

the HYPOTENEWS

Graduating senior Carl McTague won the 2004 McKibbin medal, awarded annually by the Arts and Sciences faculty to the one who, in scholarship, character, and promise in his chosen field, is considered the most outstanding graduating man. During his senior year, Carl worked on the topology of spaces with singularities under the direction of topologist Markus Banagl. His project aimed to develop techniques for computing hypercohomology on a computer by means of combinatorial sheaves, in order to study stratified pseudomanifolds. Carl begins graduate study at Cambridge University in England this fall.

remembering ARNO JAEGER



Arno Jaeger, professor of mathematics at UC from 1953-1970, died on February 28, 2004, at the age of 82. News of his death inspired his former student and current UC faculty member, Roger Chalkley, to reminisce on Jaeger's accomplishments and his role in the history of the UC department of mathematical sciences.

The death of Arno Jaeger will recall to many of his former students and colleagues his kindness, wisdom, and extensive experience. A child actor and newspaper editor in his youth, he worked nonagressively for the Luftwaffe on the development of radar during World War II. He became a prisoner of war and used that time to study mathematics. After earning his PhD (Dr. rer nat) from the University of Göttingen in 1949, he pursued postgraduate studies at the University of Manchester. He was director of a graduate program in mathematics at the University College Ibadan in Nigeria during 1950-1952, a research associate at the University of Illinois in 1952, and in 1953 was appointed as a member of the graduate faculty at UC to replace Otto Szasz. He returned to Germany in 1970.

When Arno Jaeger arrived in Cincinnati, his research interests included differential algebra, and that influenced the theses of his first three PhD students (Frank Levin in 1956, Roger Chalkley in 1958, and William Larkin in 1961). His interests in linear programming, algebra, and operations research influenced the theses of his five later PhD students at UC (Bertram Mond in 1963, Yueh-er Kuo in 1964, Ralph Fairchild in 1966, Gerald Shawhan in 1966, and Ali Khatib in 1967). He was a pioneer in introducing linear algebra as a lower level undergraduate subject. In 1960, he published his linear algebra textbook, *Introduction to Analytic Geometry and Linear Algebra*, one of the earliest written for American students at the freshman or sophomore level.

The mathematics department did not exist in its current form when Dr. Jaeger arrived. Instead there were three separate departments. (i) There was the large mathematics department of the College of Engineering that had been headed by Dr. Louis Brand during the years 1931—1956. Its members taught all of the courses on mathematics, mechanics, descriptive geometry etc. taken by students of engineering. The required sequence of courses for engineering students was arranged quite logically, and standards were enforced impersonally as if by an army. (ii) There was the much smaller mathematics department for the College of Liberal Arts (later renamed Arts and Sciences) headed by Dr. Gaylord Merriman. It consisted of Dr. Merriman, Dr. Isaac Barnett, Dr. David Lipsich, Miss Jean Winston, and an instructor (e.g., Chalkley in 1957-1958). (iii) There was the graduate faculty consisting of Dr. Brand, Dr. Jaeger, Dr. Barnett, and Dr. Wolfgang Jurkat or Dr. Alexander Peyerimhoff in alternate years (both former students of Konrad Knopp), Dr. Russell Dunholter, Dr. Clarence Lubin, Dr. Meyer Salkover, and several others.

Our present mathematics department evolved from the three earlier ones through a series of compromises and political events. Dr. Brand was appointed administrative head of all three departments shortly before his compulsory retirement at age 70 in 1956. (Dr. Brand went on to teach mathematics at the University of Houston after age 70 and won several teaching awards there in different years. At UC, there is now no mandatory retirement.) Upon Dr. Brand's retirement, Dr. Merriman became administrative head of all three departments. Dr. Merriman suffered a stroke, and Dr. Lipsich took over his duties as head. After UC became a state university in 1963, the semester system of the Liberal Arts College and the cooperative-student calendar of the College of Engineering were merged into the present quarter system. Then students in both colleges could be taught by professors in both. The emphasis of Drs. Lipsich, Jaeger, Wagner, and Merkes on pure mathematics allowed Ron Huston, Louis Doty, and the numerous other members of the engineering faculty to concentrate on teaching mechanics and other applied courses. Calculus and other math classes for engineering students were then taught by the remaining faculty.

The '60's were a time of great change for the department. As some will recall, class sizes in calculus increased from fewer than 30 students to 80-90 or more by the late 1960's. The need for additional faculty resulted in the hiring of young PhD recipients as opposed to the practice of hiring a few experienced researchers as graduate faculty. Research became very specialized. The PhD oral examination in which all the members of the graduate faculty were present to ask any mathematical questions that could expose obvious weaknesses in candidates was discontinued. Since the state provided a subsidy for each PhD degree awarded, young faculty members were encouraged to serve as PhD thesis advisers, and this greatly increased the output of degrees. Arno Jaeger deplored the consequent lowering of standards; but before supply and demand later dictated more realistic output of PhDs, he returned to Germany in 1970 to assume a professorship at the Ruhr University in Bochum Germany. There he married, became a father, and continued his research pursuits. He experienced some disappointments along the way, divorced, and suffered a stroke in 1993. In 1998, he married Dr. Charlotte Jaeger. Throughout his life he traveled extensively, visiting Australia, China, Japan, Egypt, India, Peru, Bolivia, Argentina, Mexico, and all European countries. He took numerous photographs and mailed many postcards with unusual stamps to his former students and colleagues. His last visit to Cincinnati was in 1992. In 1997, he published his autobiography about a life filled with many interesting encounters and accomplishments: *Mathematik und Leben – eine seltene Gleichung: Memoiren eines Hochschullehrers auf vier Kontinenten*.

THE RIGHT ANGLE is produced by the Department of Mathematical Sciences McMicken College of Arts and Sciences University of Cincinnati PO Box 210025 Cincinnati, OH 45221-0025

THE RIGHT ANGLE

Editor: Joanna Mitro
For more information, call (513) 556-4050 or email us at RightAngle@math.uc.edu
Comments and suggestions are welcome.

Layout and design by McMicken College of Arts and Sciences Office of Marketing and Communications

Please affix postage here

THE RIGHT ANGLE
Department of Mathematical Sciences
McMicken College of Arts and Sciences
University of Cincinnati
PO BOX 210025
Cincinnati, OH 45221-0025

F O L D H E R E

from the EDITOR

The Right Angle is our best way to keep you informed about happenings in our corner of the world of mathematics. I hope you've enjoyed this issue. Please use this form to keep us up to date on your happenings, too.

Joanna Mitro

Name _____
Address _____
_____
Year of graduation _____
Degree _____
Current occupation _____
Professional or personal news (comments/suggestions):
_____
_____
_____
_____
_____
_____

introducing XIAODONG LIN

After spending a year as postdoctoral visitor at the Statistical and Applied Sciences Institute in Chapel Hill, NC, Xiaodong Lin joins the department this fall as an assistant professor. He obtained his PhD in statistics from Purdue University in 2003. He also has an MS in statistics with a concentration in computational finance and an MS in computer science from Purdue. His main research interests are data mining, machine learning and statistical learning theory. We asked Xiaodong to provide an overview of the new field of data mining. He says the following.

Data mining is concerned with the ability to make sense of data. In many fields, data are being collected and accumulated at a dramatic pace. In astronomy, for example, terabytes of image data are collected daily to study the classification and cataloging of sky objects. (Editor's note: a terabyte is a trillion (10^{12} bytes) Because of the scale of such data sets, traditional analysis tools can no longer be applied. There is an urgent need for a new generation of computational theories and tools to assist in extracting useful information (hidden patterns, relationships etc.) from the rapidly growing volumes of data. These theories and tools are the subject of the emerging field of data mining and knowledge discovery.

Data mining is an evolving interdisciplinary field connecting statistics, machine learning, pattern recognition, databases and high performance computing. The process is complicated and dynamic, beginning with data collection, management, and preprocessing. Many traditional statistical methods for data cleansing are still used, such as outlier detection and procedures to eliminate or reduce noise. Since each item in the database might be described in terms of many attributes or variables, the data set can be high-dimensional. Data reduction and projection are used to achieve a more condensed representation for the data, which leaves important features invariant. (For example, if "height" and "weight" are two variables, we may be able to combine them into the single variable "size.") The core step for data mining involves repeated iterative application of particular data analysis algorithms. Classification, regression, clustering, association rules, and dependency modeling are among the most popular ones. For example, an association rule might tell us what proportion of shoppers who purchased an item such as a jar of prepared spaghetti sauce also purchased another such as ground beef and what proportion of all shoppers purchased both.

The field of data mining not only challenges us to find new data analysis algorithms, it also generates many theoretical problems. For instance, one common type of dataset is called "short-fat." In this kind of data, the dimension (number of variables) in the dataset is close to or even higher than the sample size (number of observations). Classical asymptotic results are no longer applicable, so investigations are underway to determine the limiting properties of various statistical procedures for "short-fat" data, as both the sample size and dimension increase to infinity.

After nearly 10 years' development, data mining has provided a complex but manageable tool box for industry, research institutes, and government agencies. With the help of these tools, data mining technologies have been applied to virtually every corner of our lives, including analyzing data collected from DNA microarray experiments, managing large investment portfolios, and helping the U.S. Treasury Financial Crimes Enforcement Network identify financial transactions that might indicate money-laundering activities. With interesting issues related to the development and study of complex methodology and driven by such a large number of applications, data mining will continue to be an important research field in the years to come.

THE RIGHT ANGLE
Department of Mathematical Sciences
McMicken College of Arts and Sciences
University of Cincinnati
PO Box 210025
Cincinnati, OH 45221-0025

RETURN ADDRESS REQUESTED

0351

Non-profit
Organization
U.S. Postage
PAID
Permit No. 133
Cincinnati, OH

THE RIGHT ANGLE

Vol. 12 MATHEMATICS ALUMNI NEWSLETTER Autumn 2004

McMICKEN COLLEGE OF ARTS AND SCIENCES
Department of Mathematical Sciences
RightAngle@math.uc.edu

UNIVERSITY OF Cincinnati

from the HEAD

Thanks again to the many friends of the department for their continuing support. We are particularly grateful to the Barnett family for their generous support of the annual Barnett Lecture. This year's lecture by Wolfgang Pollack on quantum computing attracted a particularly large audience including faculty and students from physics and engineering.

This was a banner year for external funding for our department. Particularly notable were grants from the National Science Foundation to Nages Shanmugalingam for her work on geometric function theory and from the National Security Agency to Magda Peligrad for her work on probability. Dave Minda, Chuck Groetsch and Joy Moore received a large grant from the National Science Foundation for further education of high school teachers. They are part of a syndicate centered at the Institute for Advanced Study in Princeton.

Three members of the departmental family embark on divergent paths as the new academic year begins. Assistant Professor Markus Banagl is leaving to join the faculty at the University of Heidelberg, Germany; Carl McTague, one of the department's most accomplished undergraduates, moves on to study at Cambridge University after winning the college's McKibben medal. Sue Curtis, the department's office manager since 1988, retires in September after 30 years of service to the university. We wish them well in their new pursuits.

Congratulations to alumnus Dennis Berkey who was recently chosen to be the president of Worcester Polytechnic Institute. Dr. Berkey received his PhD in mathematics at UC in 1974.

The completion of the Collegiate Restructuring Initiative has resulted in significant changes to the department. We will be taking over a number of classes such as College Algebra and Business Calculus that were formerly taught by University College. To help with the increased instructional load, eight new faculty will join us this year. They include Ning Zhong from Clermont College and Connie Roth and Mihaela Poplicher from University College. Plans are also underway for an expanded Mathematics Help Center in 614 Old Chemistry. The center will focus on providing support for students in first and second year classes.

Best wishes for a pleasant and productive year,

T. J. Hodges

Tim Hodges

keeping SECRETS

The need for encryption has been with us for centuries. One simple form of encryption, repeatedly discovered by generations of children, is the substitution method, where one set of symbols is substituted for another. The key to encrypting or decrypting a message in this case is a chart showing the correspondence between the sets of symbols. This is a form of symmetric key cryptosystem: the two parties who want to communicate securely must both possess the same private or secret key.

Throughout history, more and more complex ciphers and coding systems have been devised, eventually necessitating machines and, more recently, computers to do the actual encryption and decryption. However, the need to exchange keys between parties who want to communicate confidential information began to present an enormous logistical burden. The search for a solution to the problem of key exchange led to the revolutionary idea of public key cryptosystems. In a public key cryptosystem, the key consists of two different parts, a public key and a private key. The public key is accessible to anyone, and it is used either to encrypt a message or to verify the authenticity of an electronic signature. The secret key is used either to decrypt a message or to produce an electronic signature. That is, the private key is used to produce a digital signature which can be verified as authentic using the public key. This asymmetric design allows one to communicate securely over an open communication channel without any prior exchange of a secret key. Public key cryptosystems are now widely used to provide security and privacy in the Internet and throughout society. The first protocol for a public key exchange was envisioned in 1976 by Diffie and Hellman. The widely-used RSA cryptosystem of Rivest, Shamir, and Adleman is the first practical realization of a public key cryptosystem.

Roughly speaking, the security of the RSA type of cryptosystem relies on the difficulty of factoring integers. In this system, one chooses two large primes p and q. The public key consists of the integer $N = pq$ together with a number e which is relatively prime to $(p\text{-}1)(q\text{-}1)$. Messages to be transmitted are converted to a string of numbers (each assumed to be less than N), and then each number is encoded by $n \longrightarrow m = n^e \pmod N$. In this case the secret key s has the property that for any integer b, $(b^e)^s = b \pmod N$. Thus raising the encoded number to the power s reverses the encryption. From elementary number theory, we know the number s can be characterized by the property $se = 1 \pmod{(p\text{-}1)(q\text{-}1)}$. If the factors p and q are known, s can be computed using the Euclidean (division) algorithm. Thus for this encryption method to be considered secure, N should be large enough (at least 1024 bits—or roughly 340 decimal digits) to defeat the attempts of super computers (or millions of personal computers working together) to discover its prime factors. Unfortunately, the large size of N also necessitates a huge amount of calculation in the encryption process, making communication slow and inefficient. In practical communication systems, public key systems never stand alone. They are often used to exchange keys for a symmetric cryptosystem.

> Suppose $N = 77 = 11 \times 7$ and $e = 7$ (which is relatively prime to $60 = (11\text{-}1) \times (7\text{-}1)$). The secret key in this case is $s = 43$.
> Note: $7 \times 43 = 301 = 1 \pmod{60}$.
> The message $n = 36$ is encrypted as $m = 36^7 \pmod{77} = 64$.
> To decrypt this message, one must compute $64^{43} \pmod{77}$.

Recently an unexpected threat to the RSA system appeared. Peter Shor of AT&T Labs developed a polynomial-time algorithm for factoring integers on a quantum computer. This means that if a quantum computer can be built, the RSA systems would no be longer secure. Although we still do not have suitable quantum computers, a tremendous amount of effort is being devoted to developing them, in part because of their tremendous code-breaking potential. Some researchers seek new ways to program such a machine. Others are motivated to search for more efficient and secure cryptosystems. Currently Professor Jintai Ding and his students are working in this direction.

The search for new public key cryptosystems has led to elliptic curve cryptosystems, lattice cryptosystems, and multivariable cryptosystems. Each system exploits a computationally difficult problem in an area of mathematics. The RSA system explained above is based on number theory, mathematics developed in the 17th and 18th centuries. Elliptic curve cryptosystems are based on the mathematics of elliptic curves, mathematics of the 19th century. Multivariable cryptosystems are built using multivariable polynomials and are based on algebraic geometry, mathematics developed in the 20th century. These latter systems have been the focus of Ding's research group.

Professor Jintai Ding

In multivariable cryptosystems, the message to be encrypted is first translated into a string of elements in some finite field K—e.g., integers modulo a prime number. The encryption is accomplished by applying a function (the public key) which is easy to store and compute. The output of this function is the ciphertext (also a string of elements of K). Decryption amounts to solving a set of general multivariable polynomial equations over finite fields. Jintai explains that the method used to solve such a system, known as the Groebner Basis Method, is of exponential complexity (comparable to integer factorization on today's computers), so there is no efficient algorithm. However, the function used in these systems is the composition of several simple maps, and the private key consists of knowledge of the composite components. This knowledge allows the recipient to decipher the message. Security of the cipher is based on the inherent difficulty (impossibility) of factoring composite multivariable maps. (This is the subject of the famous Jacobian conjecture about invertible maps.) Last year, Ding applied for a patent on a multivariable cryptosystem he designed using novel elements in the composition process.

Each new cryptosystem poses a challenge to mathematicians and computer scientists—can an algorithm be found to break it? For example, the Sflash scheme, chosen as a European security standard for implementation on low-cost smart cards, is an application of a multivariable cryptosystem. Recently Jintai Ding, working with professor of computer science Dieter Schmidt, found a security weakness in its newest version (Sflash-v3), due to its algebraic structure. Jintai Ding, his student, Zhijun Yin, and Dieter Schmidt worked together to break the TTS cryptosystem. Jintai Ding, Dieter Schmidt, and Timothy Hodges succeeded in breaking the TTM cryptosystem. New designs, like the one proposed by Ding, avoid known pitfalls and are getting stronger.

The theory behind multivariable cryptosystems has matured quickly in the last decade. With the increasing use of electronic communications for data transmission and the proliferation of electronic devices for data storage, there exists great potential for the practical applications of these ideas. In addition, there are still many unsolved mathematical problems in this area. New mathematical insights, especially insights from algebraic geometry, will be fundamental in dealing with these problems.