The Quaternion

Volume 31: Number 1; Fall, 2016
The Newsletter of the Department of Mathematics and Statistics

UNIVERSITY OF SOUTH FLORIDA

Contents

Mathematics and Cybersecurity at USF 1
Transition 3
Departmental News 3
Faculty News 4
Student News 4

Mathematics and Cybersecurity at USF

The Internet may have been a curiosity in the Twentieth century, but now it's a major part of the economy. According to the McKinsey Global Institute, in 2009 the Internet accounted for 3.4 % of the world's economic activity, more than education or agriculture. According to the Boston Consulting Group, in 2010 the Internet accounted for 4.7 % of the US economy, more than the federal government. The Internet is growing about 10 % a year, and that attracts a wide variety of entrepreneurs. That includes criminals.

As the old line goes, Willie Sutton robbed banks because that's where the money was. Now the money's on the net, so that's where robbers go. And spies, saboteurs, and vandals. In 2014, McAffee estimated that "cybercrime" costs the world economy about half a trillion dollars a year. Hence the demand for "cybersecurity."

The Florida state government responded by creating the *Florida Center for Cybersecurity* (fc^2), based at the University of South Florida, with supporting programs throughout the State University System. The USF program is a *National Center for Academic Excellence in Cyber Defense*, with baccalaureate and masters' programs certified by the National Security Agency. It includes a program for preparation for *the Certified Information Systems Security Professional* (CISSP) certificate.

This is an interdisciplinary program, spanning the colleges of Arts & Sciences, Behavioral & Community Sciences, Business, Education, and Engineering. "Demand is so large that there will be two hundred thousand positions that will go unfilled" this year, said fc^2 Managing Director **Sri Sridharan**, who anticipates one to two million new cybersecurity jobs during the next three years. That includes jobs in law enforcement, from local police to the FBI and Secret Service, to IT jobs in corporations and institutions.

Mathematics is a source of much of the cybersecurity toolkit. And USF is developing the next generation of tools.

Kaiqi Xiong works on securing networks - networks of computers that are invisible to the user. This is convenient for users who want to avoid the machine-dependent details. One such convenience is the *Software Defined Network* (SDN), which is a system pretending to be the network that the user desires. The system mimics the desired network, handling the details itself. Possible applications range from airline traffic to currency transactions; the former application shows the stakes in getting the programming right - and the latter shows the opportunities for spies and saboteurs.

For example, machines in the SDN system communicate by sending messages, and the virtual machines that they mimic communicate by sending messages. A hacker might gain access by tricking a participating machine to open and act on a spurious message.

This happens in email all the time: a criminal sends a legitimate-looking email with a "Trojan" - a piece of code that sneaks in with the email. The Trojan might steal secrets, sabotage or take over the

Continued on page 2

The Quaternion is an annual publication of the USF Department of Mathematics & Statistics, which can be visited on the web at `<http://www.math.usf.edu/>`. Our our snail-mail address is Department of Mathematics and Statistics, University of South Florida, 4202 E. Fowler Ave., CMC342, Tampa, FL 33620-5700. Our phone number is (813) 974-2643, and our fax number is (813) 974-2700.

Mathematics and Cybersecurity at USF

Continued from page 1

computer, or even hold it for ransom. There is no absolute test to check if an email contains a Trojan: in 1989, William Dowling observed that from Rice's Theorem it follows that no such absolute test can exist. We are stuck in a perpetual arms race with the hackers.

Professor Xiong works on the question: upon receipt of a message allegedly sent by goodmachine.org, what does one do with it? Servers handling messages need increasingly sophisticated tests to detect increasingly sophisticated hacks, while not blocking legitimate messages needed to keep the network running. That's why servers encrypt their messages so that legitimate messages are accepted while illegitimate messages are not.

Encryption is part of cryptography, the mathematical foundation for engineering secure computing and communications systems and protecting them from hacks. The underlying model of encryption is to allow two people to communicate over a possibly compromised channel, but so that a third party would not be able to decode an intercepted message (or create a usable spurious message). The Department of Mathematics & Statistics has an active cryptography group.

Jean-François Biasse and **Dima Savchuk** use groups to encode messages. A *group* is a collection of objects, like numbers, matrices or permutations, which can be combined to get other objects of the group. (A group also has an identity and inverses.) The set of all positive fractions using multiplication is a group; the set of all real numbers under addition is a group.

Groups have been used in encryption for some time. For example, the Diffie-Hellman-Merkle "open key" method for two people to openly agree to a code while frustrating spies. Let G be a group, and let $g \in G$. Jack chooses a secret number x and sends the power g^x to Jill; the spy might intercept g^x but would have difficulty computing x. Meanwhile, Jill chooses a secret y and sends g^y to Jill. Jack can compute $(g^y)^x = g^{yx}$ and Jill can compute $(g^x)^y = g^{xy}$ and if $g^{xy} = g^{yx}$, Jack and Jill have a shared key that a spy cannot readily get from the intercepted g^x and g^y.

But many experts, including the U. S. Department of Commerce, anticipate a quantum leap in the arms race with hackers. Quantum computers - computers whose circuits can be in "mixed" states (partially OFF and partially ON) rather than current computers (whose circuits are either in state OFF or state ON) - are moving off the drawing board and into the laboratory. Some experts anticipate commercially viable quantum computers within five to fifteen years. And it looks like quantum computers will be able to readily crack our favorite cryptographic systems.

Professors Biasse and Savchuk are working on cryptographic systems that should be less vulnerable to quantum computing attacks. For example, one kind of commutative group Professor Biasse has worked with is a *geometric lattice*. Suppose you wanted to send a message consisting of the list (4, 11, -3, 9, 0, 2). If you had a *basis* of six-dimensional vectors - say, $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4, \mathbf{b}_5, \mathbf{b}_6\}$ - you could transmit the sum $4\mathbf{b}_1 + 11\mathbf{b}_2 - 3\mathbf{b}_3 + 9\mathbf{b}_4 + 0\mathbf{b}_5 + 2\mathbf{b}_6$, and the recipient could readily decode the message if the recipient had that basis. A spy who intercepted the message but did not have the basis would have difficulty decoding the message - even with a quantum computer.

On the other hand, Professor Savchuk has been working with *noncommutative* groups. Addition and multiplication are *commutative* in the sense that $A + B = B + A$ and $A \times B = B \times A$. But the set of all one-to-one and onto functions of the real numbers under composition is a noncommutative group. For example, if $f(x) = x^3$ and $g(x) = x+1$, then $(f \circ g)(x) = f(g(x)) = (x+1)^3 \neq x^3+1 = g(f(x)) = (g \circ f)(x)$. Then using noncommutative groups, Jack and Jill could send (carefully selected) elements $x^{-1}gx$ and $y^{-1}gy$ back and forth, again presenting difficulties for a hacker armed with a quantum computer.

Biasse and Savchuk also teach a course, *Introduction to Cryptography and Coding Theory*, recently launched at USF. Coding theory is different form cryptography: how to handle messages that have been degraded by interference. (Coding theory is of great interest to NASA, which

Continued on page 3

Mathematics and Cybersecurity at USF

Continued from page 2

has to communicate with robots billions of miles from Earth.) Meanwhile, they are developing the foundations for securing keys and keeping ahead in the arms race with the hackers.

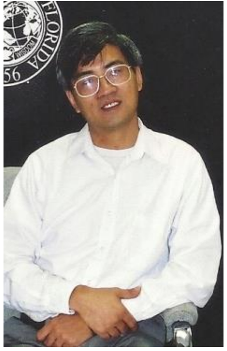
The demand for cybersecurity is only going to increase, and USF will be at the forefront of meeting this demand.

Transition

Xiang-dong Hou has stepped down as Graduate Program Director after five years. He is succeeded by **Brian Curtin**. We thank Professor Hou for his service.

Lu Lu has been reassigned as a tenure-track assistant professor. She received her Ph.D. in statistics from Iowa State in 2009, and a post doc at Los Alamos, USF hired her as a visiting assistant professor in 2013.

Dima Savchuk was awarded tenure and promoted to associate professor.



Stephen Suen has retired after 23 years at USF. A student of Geoffrey Grimmett at the University of Bristol, he applied probabilistic methods to solve problems in combinatorics and algorithms, particularly in graph theory. In 2014, he became Associate Chair. We wish him well on his future adventures. Meanwhile, **Scott Rimbey** is returning to the Associate Chair's office.

This August was the golden (fiftieth) anniversary for **Marcus McWaters**, who came to USF in 1966. He is one of two USF faculty who have served half a century at USF.

Rebecca Wooten has left the University of South Florida after 25 years, first as a tutor for Project Thrust and a graduate student, later as an adjunct and then an assistant professor. A student of **Chris Tsokos**, she continued her work in applied statistics at USF while helping out in the Urban Scholars Outreach Program and many other efforts. We wish her well on her further adventures.

Departmental News

The Department is the home for a new interdisciplinary **Center for Complex Data Systems** (CCDS), under the direction of **Les Skrzypek** and affiliated with faculty of the departments of Chemistry, Economics, Geosciences, and Physics, as well as Research Computing. It has started a new Distinguished Scholar Lecture Series, and this spring invited Marius Stan (of the Argonne National Laboratory, the University of Chicago and Northwestern University), James Hyman (Philips Distinguished Professor at Tulane University and past president of SIAM), and Edriss Titi (of Texas A & M and the Weizmann Institute of Science).

The Department also participates in an **Interdisciplinary Data Sciences Consortium**, directed by **Kandethody Ramachandran**, whose board spans four colleges as well as local firms and the Center for Disease Control and Prevention. In 2015, it invited four speakers to make presentations.

The **STEM Education Center** held the 38th annual **STEM for Scholars** summer program for 44 gifted high school students last July. The American Mathematical Society, the Jacarlene Foundation, the Academy of Applied Science/Army Research Office and the Citi Women in Technology Group provided $ 19,400 for scholarships. The courses offered were in *Microbiology* (by **Lindsey Shaw** of Cell, Molecular and Micro Biology), *Advanced Mathematics II* (by **Razvan Teodorescu**, who mentored Roshan Warman, and Warman received the AMS *Ky and Yu-Fen Fan Award*), Introduction to Calculus (by **Manoug Manougian**), Intelligent Robots (by **Yu Sun** of CSEE), and *3-D Visualization* (by **Howard Kaplan** of *Electrical Engineering* and **Steven Fernandez** of Public Affairs).

Continued on page 4

Departmental News

Continued from page 3

The Department and the Pi Mu Epsilon honor society hosted the two Hillsborough County Math Bowls during the last academic year. **Fernando Burgos** and **Paul Thorne** (for the high schools), assisted by Fred Zerla, oversaw the bowls. Both times, King High School took first place.

Ken Ono, the Asa Griggs Candler Professor of Mathematics at Emory University, delivered the Kent Nagle Lecture last March. He spoke on the life and work of Srinivasa Ramanujan, an amateur mathematician who developed some of the deepest mathematics of the 20th century. Ono was an associate producer for the 2016 biographical film *The Man Who Knew Infinity*, starring Dev Patel as Ramanujan.

L to R: Jeffrey Nagle, Ken Ono, and Sandra Nagle.

The Nagle Lecture Series was established in honor of the late R. Kent Nagle, who was deeply interested in mathematics in scholarship, education and society.

Faculty News

Jean-François Biasse was awarded a five-year $ 35,000 grant from the Simons Foundation for project in *Algorithms in Number Theory, Quantum Information, and Cryptography*.

Arthur Danielyan, **Seung Yeop Lee**, **Razvan Teodorescu**, and **Sherwin Kouchekian** received a $ 25,000 NSF grant to host 32nd Southeastern Analysis Meeting at USF.

Dima Khavinson and **Catherine Beneteau** received a $ 25,000 NSF grant to organize an international summer school on *Spectral Theory and its Applications* that was held at the University of Laval in Canada.

Wen-Xiu Ma was on Thomson Reuters' 2015 *Highly Cited Researchers* list.

Manoug Manougian was invited to the *Global Aerospace Summit* in March at Abu Dhabi.

Vilmos Totik was elected a fellow of the American Mathematical Society "For contributions to classical analysis and approximation theory and for exposition."

Kaiqi Xiong received $ 750,000 from BBN Technologies and the National Science Foundation for cybersecurity research and education.

We also have a picnic every fall. From left to right, Alan Sola (now at Stockholm University), Mile Krajcevski, Fernando Burgos, and Dulce Garcia.

Student News

The USF Chapters of the Mathematical Association of America and Pi Mu Epsilon honor society met biweekly over pizza this last year, where they heard presentations by faculty and students. Math club members attended the 2015 MAA Suncoast Meeting at Florida Polytechnic University on December 4 and the 2016 MAA Florida Section Meeting on February 26 & 27 at St. Leo University.

Continued on page 5

Student News

Continued from page 4

Lukas Nabergall made a presentation on *Patterns and Distances for Double Occurrence Words* at the Section Meeting. During that year, **Nicole Hudson** served as President of the Math Clubs, and **Anjanet Loon** as Vice President.

Sixteen students were inducted into Pi Mu Epsilon in April: **Corinne Barnes**, **Nathan Callihan**, **Anthony Cilluffo**, **Jennifer Cuartas**, **Kevin Dennis**, **Grace Gardner**, **Jennifer Gronek**, **Nicole Hudson**, **Carrie Ann Jessell**, **Elizabeth Loisel**, **Angelica Lim**, **Kevin Martinez**, **Michael Putnam**, **Benjamin Stortenbecker**, **Allison Talley**, and **Xiaoqi Wen**. Many attended the Pi Mu Epsilon Banquet. Last year, the president of the USF Chapter of Pi Mu Epsilon was **Andres Saez** and the vice president was **Kara Heuer**.

In addition, **Benjamin Stortenbecker** and **Lukas Nabergall** were this year's Outstanding Scholars:

Mr. Stortenbecker then presented his paper on *Electron Jamming through Spectral Theory* at the 2016 Pi Mu Epsilon National Meeting in August.

Meanwhile, **Brian Hunter Jackson** won $ 10,000 at the third annual *Healthcare Innovation Competition* for a proposal to manage disease pathology using cloud-based computer analysis.

2015 Third Annual State of Florida Healthcare Innovation Competition
Pay to the Order of
1st PLACE WINNER
$10,000
Ten thousand
Dollars
Sponsored by:
Florida Blue
USF
CENTER FOR ENTREPRENEURSHIP
NAI

During summer and fall, 2015, and spring, 2016, sixty student received their BAs: **Zuhair Al-Abbasi**; **Connor Alkhatib**; **Dylan Allen**; **Corinne Barnes**, *Summa Cum Laude*; **Christopher Bello**, *Magna Cum Laude*; **Sarah Branthoover**, *Magna Cum Laude*; **Shannon Cunningham**, *Magna Cum Laude*; **Terri Davis**; **Rahul Dudhat**; **Timothy Freeman**, *Magna Cum Laude*; **Ricky Godinez**; **Isamar Gonzalez Torres**, *Magna Cum Laude*; **Johnathan Gray**, *Magna Cum Laude*; **Jennifer Gronek**; **Alexander Hagen**, *Cum Laude*; **Hayley Hall**; **Mehrez Hannachi**, *Cum Laude*; **Suzzanne Harmon**, *Magna Cum Laude*; **Ryan Hatter**; **Jamie Heath**, *Cum Laude*; **Kristine Heburn**; **John Heise**, *Cum Laude*; **Ryan Hensel**; **Derek Hicks**; **Donald Hood**, *Magna Cum Laude*; **Tyler Iorizzo**, *Magna Cum Laude*; **Brian Jackson**; **Katherine Japour**; **Denys Kukushkin**, *Summa Cum Laude*; **Melissa Kurtz**, *Magna Cum Laude*; **Faith Martin**, *Summa Cum Laude*; **Roger Matthews**; **Wenjun Meng**, *Summa Cum Laude*; **Edward Mitchell**; **Laura Mockensturm**, *Magna Cum Laude*; **Erik Newhard**; **Erica Nunn**, *Magna Cum Laude*; **Jamie Pardasie**; **Ashley Parisi-Goldblatt**; **Jackson Pawson**; **Edwin Peguero**, *Magna Cum Laude*; **Allen Pennington**; **Minh Pham**, *Summa Cum Laude*; **Daniel Reinhard**, *Cum Laude*; **Julia Rich**; **Freida Rivera**; **Ricardo Romeu-Kelly**, *Magna Cum Laude*; **Luis Sanabria**; **Samantha Sayers**; **Matthew Sherlip**; **Tooba Siddiqui**; **Amber Sierra**; **Kierstin Simmons**, *Magna Cum Laude*; **Benjamin Stortenbecker**, *Magna Cum Laude*; **Erika Tate**; **Elizabeth Toth**, *Magna Cum Laude*; **Alisa Vasserman**, *Summa Cum Laude*; **Richard Warner**, *Summa Cum Laude*; **Jeffrey Winny**, *Cum*

Continued on page 6

Student News

Continued from page 5

Laude; and **Bruce Wong**.

Twelve students received MAs: **A. K. M. Bashar**; **Wei Chen**, *Analysis of Rheumatoid Arthritis Data Using Logistic Regression and Penalized Approach* under **Dan Shen**; **Gregory Churchill**; **Jeremy Kerr**, *On the Number of Colors in Quandle Knot Colorings* under **Mohamed Elhamdadi**; **Shanna Lindemeyer**; **Josiah Park**, *Generalized Phase Retrieval: Isometries in Vector Spaces* under **Boris Shekhtman**; **Jonathan Spiewak**, *Leonard Systems and their Friends* under **Brian Curtin**; **Yue Sun**, *Resonant Solutions to (3+1)-Dimensional Bilinear Differential Equations* under **Wen-Xiu Ma**; **Hongliang Wang**; **Tae Hyon Whang**; **Yun Yun**; **Xiaochuang Zhao**, *Ensemble Learning Method on Machine Maintenance Data* under **Dan Shen**.

And three students received PhDs: **Joy D'Andrea**, *A Statistical Analysis of Hurricanes in the Atlantic Basin and Sinkholes in Florida* under **Rebecca Wooten**; **Venkateswara Mudunuru**, *Modeling and Survival Analysis of Breast Cancer: A Statistical, Artificial Neural Network, and Decision Tree Approach* under **Lesław A. Skrzypek**; and **Vindya Pathirana Arachchilage**, *Nearest Neighbor Foreign Exchange Rate Forecasting with Mahalanobis Distance* under **Kandethody Ramachandran**.