“Imagine the U.S. Open, except the participants are not humans but ciphers.”

Kris Gaj, Associate Professor, Cryptographic Engineering Research Group

Battles of Cryptographic Algorithms

Kris Gaj’s interest in math and computers led him to cryptography—the science of developing and breaking ciphers. As one of his undergraduate summer projects at Warsaw University of Technology in Poland, he took on the mathematical and engineering foundations of breaking German Enigma cipher. This work had been done by Polish cryptologists, several years before the start of World War II. He was inspired by their incredible breakthrough, accomplished years before any attempts by Alan Turing and his Bletchley Park colleagues, depicted in the recent Oscar-nominated movie The Imitation Game. This memorable summer led to Gaj’s first major computer program—a visual simulator of Enigma, as well as his first major publication—a comprehensive report, turned into a book, published a year after he graduated from college.

However, Gaj did not want to focus on the past; he wanted to apply its lessons to the present and future. He pursued a PhD on modern cryptographic schemes and their efficient implementations, and, with a group of friends, started a company developing cryptographic software and hardware for major Polish banks and government institutions.

After the company got off the ground, he decided to pursue his dream of working as a researcher and professor in the United States. For three years, he worked as a postdoctoral student at the University of Rochester in the area of CAD tools for high-speed electronics, and then in 1998, applied for a tenure-track position at Mason.

Continued on page 8
Dear Alumni and Friends,

As our school continues to grow, our goal is to raise our international visibility to attract some of the world’s best international students, and to open doors for international research and collaboration with other universities. This fall we took some big steps in that direction.

As we approached the month of December, many faculty in ECE at George Mason were very busy organizing and running two IEEE flagship conferences. The first, GLOBECOM 2016, one of two flagship conferences of the IEEE Communications Society, is expected to have up to 2,500 attendees. The conference was held in the Washington Hilton from December 4 to 8 and the general chair was Professor Bijan Jabbari. The second is GlobalSIP 2016, a flagship conference of the IEEE Signal Processing Society that was held at the Crystal Gateway Marriott from December 9 to 12, with Professor Gerry Tian (ECE at Mason) and Brian Sadler (Army Research Laboratory) as the general chairs.

Also during the fall I personally traveled to a variety of international venues to promote our department, school, and faculty. My journey began with a conference in Lecce, Italy, to present some of our research on machine learning. I then traveled to Korea to give an invited plenary talk at the Acoustical Society of Korea’s meeting in Gyeongju and later to give a seminar and meet faculty and students at Korea University in Seoul. The next stop was Shenzhen, China, for a visit to the Georgia Tech-Shenzhen campus to give a talk and meet graduate students. A few weeks later, I was in Cancun to present more of our research in machine learning. By the end of these trips, I found myself singing the classic song by Chicago, “Does Anybody Really Know What Time it Is?”

Back on the Fairfax Campus we have added new faculty to our ranks. I would like to extend an enthusiastic welcome to these three individuals who are profiled inside this newsletter: Cameron Nowzari and Feitian Zhang in electrical engineering, who have research interests in controls and robotics, and Xiang Chen in computer engineering, who is developing the Intelligence Fusion Laboratory.

I invite you to stay in touch with us by following us on Facebook, and I look forward to sharing more news and stories of our department in the future.

Monson H. Hayes
Chair, Department of Electrical and Computer Engineering
ECE alumnus Eric Nallon has been attracting a lot of attention in the field of sensors and actuators with his electronic nose (e-nose) research.

A biologically inspired device, the e-nose is designed to mimic the operation of the human olfactory system. It uses a chemical sensor array consisting of broadly responsive vapor sensors, the combined response of which produces a unique pattern for a given compound or mixture. The sensor array derives its inspiration from the biological function of the receptor neurons found in the human olfactory system.

An e-nose provides an attractive approach to predict unknown odors and is used in many fields for quantitative and qualitative analysis. If properly designed, an e-nose can adapt to new odors it was not originally designed for through laboratory training and algorithm updates, eliminating lengthy and costly research and development costs associated with material and product development. Although e-nose technology has been around for more than two decades, researchers are searching for new and more diverse types of sensors.

Nallon has used graphene as the sensing material in his research. Graphene is a single-layer, 2-D material of carbon atoms arranged in a hexagonal lattice with extraordinary electrical, mechanical, thermal, and optical properties due to its 2-D, sp2-bonded structure. The 2-D structure also provides a surface entirely exposed to its surrounding environment, giving graphene great potential as a chemical sensing material. Although graphene has gained much attention since its discovery in 2004, its use in commercial electronics remains limited.

Nallon's PhD research work incorporated graphene into a chemiresistor device and used it as a chemical sensor. In this configuration, its resistance is temporarily modified while exposed to chemical compounds, which can be monitored over time. The sensor exhibits excellent selectivity and is capable of achieving high classification accuracies. At the culmination of his work, Nallon demonstrated a first example of a graphene-based, cross-reactive chemical sensor array by applying various polymers as coatings over an array of graphene sensors. The sensor array was tested against a variety of compounds, including solvents, chemical warfare agent simulants, explosive related compounds, and the complex odor of essential oils, hot sauces, and Scotch whiskies.

A recent graduate of Mason's PhD program, Nallon earned his BS from Penn State in electrical engineering where he was introduced to semiconductors and cleanroom work for the first time. This experience opened up a whole new world of nanoscale electronics for him. When he started his master's degree and met Associate Professor Qiliang Li at Mason, he also began working on using organic polymers and organic semiconductors as materials in chemical sensors.

Nallon’s dissertation also includes the use of machine learning techniques to perform pattern recognition and classification of sensor data. He used Python and its machine-learning libraries throughout his work to process, analyze, establish patterns of, and visualize the sensor array data.

The November 2015 issue of Chemical and Engineering News featured Nallon’s work and highlighted his graphene-sensing discoveries, which had also been published by ACS Sensor in its inaugural issue. Since graduating, Nallon moved from his position at the U.S. Army’s Night Vision and Electronic Sensors Directorate and no longer works on graphene sensing (a bittersweet transition). His experience with sensor data processing and machine learning, however, helped him secure his current job as a data scientist at Commonwealth Computer Research Inc. in Charlottesville, Virginia.
NEW FACULTY

Feitian Zhang comes to the ECE Department from the Department of Aerospace Engineering and Institute for Systems Research at University of Maryland, where he was a postdoctoral research associate. Prior to his time at Maryland, Zhang earned a bachelor’s and master’s degree in automatic control from Harbin Institute of Technology and a PhD in electrical and computer engineering from Michigan State University. In his current research, he designs bio-inspired underwater robots that can maneuver in unknown and dynamic environments. A passion for teaching, research, and professional freedom led Zhang to an academic career, and he is enjoying both the flexibility and the challenge. When he’s not working, Zhang engages in sports, travel, and spending time with his family.

Xiang Chen joins the ECE Department from the University of Pittsburgh, where he completed an MS and PhD in electrical and computer engineering. His research interests are in mobile computing, mobile displays, low-power systems, and mobile security. During his PhD studies, Chen focused on low-power mobile system optimization, organic LED displays on mobile platforms, computing optimization on mobile CPUs/GPUs, and mobile security solutions. He is excited about the opportunity to research cutting-edge technology and innovation as a faculty member, and he appreciates the strong and open-minded research environment at Mason. Outside of work, Chen loves to collect video games, from old NES to cutting-edge, next-generation consoles, though he doesn’t find much time to play them.

Cameron Nowzari comes to Mason from the University of Pennsylvania, where he was a postdoctoral researcher and a lecturer. Before migrating to the East Coast, Nowzari earned a BS and PhD in mechanical engineering from UC Santa Barbara and UC San Diego, respectively. His research focuses on control of multi-agent and large-scale networked systems, and he is looking forward to teaching a new course in network control. While Nowzari was initially attracted to a PhD as a way of avoiding a “real job,” he was quickly drawn in by the freedom to set his own research agenda. In his spare time, Nowzari enjoys snowboarding, surfing, and making music. He is excited about the proximity of Mason to Washington, D.C., even though the surfing options are slim.

VISITING SCHOLAR

Insub Shin joined the Department of Electrical and Computer Engineering in 2016 as a visiting scholar and is affiliated with Mason’s C4I and Cyber Center. His research interest is in cybersecurity architecture framework for a conceptual legacy firm. This includes modeling cyber threats, organizational strategy, and systemic implementation to secure the cyberspace of an organization with a system of systems.

As a brigadier general in the Korea Army, Shin was a professor in the Department of Cyber Defense at Korea University in Seoul. Before his retirement, Shin served as secretary for cybersecurity to the president of Korea. He also served as secretary for military science to the minister of national defense of Korea, and as director of the R&D Center at the Korea Cyber Command. He received his BS in mechanical engineering from the Korea Military Academy, his MS in telecom system management from the U.S. Naval Postgraduate School, and his PhD in information technology from George Mason University. Shin has published a book and published several papers in the field of C4I and cybersecurity.
These Student Design Projects Will Be Out of This World

BY PETER PACHOWICZ, ASSOCIATE PROFESSOR

In its search for exciting frontiers for senior design projects, the ECE/VSE initiated a new CubeSat program involving undergraduate students and, potentially, graduate students. The long-term goal of this effort is for our students to launch a series of ultra-small satellites and high-altitude testbed scientific balloons.

This is a highly interdisciplinary platform for many potential engineering projects, such as spacecraft design, operations, communications, computing hardware, software, sensors, power, attitude control, testing, etc. In addition to being an educational tool, this system will also be used for testing small modules and chips in a space environment before they are used in large satellite projects.

While the concept of CubeSat is not new, the size of the satellites is shrinking rapidly as are the launching costs. The miniaturization trend continues and will test the limits of ultra-small spacecraft technology. This is why we decided to move away from a well-established PicoSat standard (10cm cube) and aim at a new concept of PocketSat (5cm cube) and the SunCube FemtoSat (3cm cube) configuration of one to three units.

This means that all components of a spacecraft must be designed from scratch and comply with space and launch environments. In the first step, a satellite communication antenna system is being designed and built to be mounted on the roof of the Nguyen Engineering Building. This system includes a 916MHz downlink, a 436MHz downlink, and a 140MHz uplink.

While the emphasis is on the development of a functional ultra-small CubeSat to be launched by students, fundamental and practical aspects of this project provide an excellent educational value. In addition, benefits for Mason include increased visibility; student excitement, which attracts high-achieving students; development of a new platform for exciting senior design projects; expansion of engineering labs; interest and sponsorship by local industry; exploration of interdisciplinary student work; and high return-on-investment due to the low cost of this initiative.
What Has Never Been Done, Can Be Done

FORMER DARPA DIRECTOR TONY TETHER SHARES EXPERIENCES, ADVICE

Editor’s note: ECE News interviewed ECE Advisory Board member and former Defense Advanced Research Projects Agency (DARPA) director Tony Tether. With his wide range of experience as an entrepreneur, a federal employee, and a government contractor, Tether observed technological change from multiple vantage points. In this interview, he offers his unique perspective on the purpose of DARPA, big ideas in science and technology, advice to future engineers, and the benefits of reading science fiction.

ECE News: Why was DARPA created and how is it relevant today?

DARPA has a very simple charter—prevent "technological surprise." DARPA was created by President Eisenhower in 1958 as a result of Sputnik. When he investigated how the USSR could have beat us into space, he found that while all services had space programs, they were not of a very high priority compared to their near-term requirements. So he created an organization with the simple charter mentioned above so such a surprise would never happen again.

I like to say that DARPA is not about showing that something can be done better, it is about proving that something that has never been done before can be done. DARPA provides existence proofs and this is still very relevant in today’s times.

You have the distinction of being the individual who had the longest tenure as a DARPA director. In the eight years you served, what makes you proudest?

There are two ideas that stand out. Exploring these ideas was surprising and challenging, and includes some of our greatest technical achievements. The first is what I call “cracking the codes of the brain,” and the second is having computers “learn” you.

What surprised us about “cracking the codes of the brain” was how simple it was—essentially the brain cracked its own codes. The technology that allowed it to occur is also one of the greatest technical achievements of the time. Microelectronics provided the ability to make wires so small they went undetected by the brain and hence were not rejected, which made it all possible.

With microelectronics, we tapped into that part of the brain that processes intent. The surprise was that we didn’t have to collect signals or do any processing. We connected a prosthetic arm to a person and asked the person to move the arm. It took a while before they could make the arm “twitch,” but the time duration from the “twitch” to having the arm move and pick up a cup and bringing it to the lips was surprisingly quick. The brain figured it out.

The second big idea was to see if computers could “learn” a person by observing—learning the person’s preferences, etc. and determine what they needed to have or do before they knew. The human equivalent was Radar O’Reilly in the TV series M*A*S*H. Radar anticipated and detected Colonel Potter’s needs and completed tasks before the colonel even asked.

My vision was that someday people would always have their computers with them wherever they went. The computer would listen in, learn, and then provide advice or take action. We are moving in that direction. Most of the current artificial intelligence involves computers learning a situation through experience, and then advising a person before even being asked.

What do you see as the biggest technical challenge of the next 10 years?

The biggest technical challenge is related to the two ideas we talked about.

We are starting to understand the human body. We are gaining a better understanding of human biology and of cancer research by putting smart things into bodies. We are entering the stage where sensors will be everywhere—the Internet of Things.

Computers will have access to all these sensors around us and will monitor all this information. They will watch us, watch over us, know all about us; the computer will have learned us. It could even call the police for us if it sensed danger.

The technical challenge will be for humans to maintain control and not have the computers control us.

SPRING 2017
Do you read science fiction?
Yes, I’m a big fan. In fact, when I interviewed prospective DARPA employees, I always asked if they read science fiction. People who write science fiction are exceptionally creative.

Science fiction writers weave facts together, extend them with imagination, and tell their stories. They are really, really innovative people, and that’s what I always looked for.

I wanted that same kind of creativity and imagination at DARPA; they were interviewing at a place where science fiction becomes real.

Was there a movie or book that gave you an idea that DARPA should explore?
Yes, the movie *2001: A Space Odyssey* had a major impact on me. In the movie, HAL was a computer that basically ran a spaceship and interacted with the crew but went rogue and took over the spaceship. I feel like I’ve been working on HAL since then.

How do you decide which projects to explore?
To define projects at DARPA, we had a process based on questions sometimes referred to as the Heilmeier Catechism named after George Heilmeier, DARPA director in the late 1970s. The first three or four questions were, in my opinion, the most important: What is the problem that you are trying to solve? If you solved it, what difference would it make? What is your approach, and how is it different from what has been tried in the past?

I still look to these questions when deciding or creating research projects.

What advice would you give to graduating or recently graduated engineers?
I would tell them to acquire a strong foundation of general knowledge along with their specialized engineering degree so they can apply their engineering education in other areas. I would tell them to become generalists instead of specialists because they don’t know what they will be doing in the future.

I would also say, “Someday you will come to a fork in the road of life, and you will need to choose which way to go.” If you have enough general knowledge, you might take the road least traveled, knowing that wherever it goes, you are confident that you will be able to handle it. If you don’t have that general knowledge, you will tend to always take the well-travelled road, missing out on creating the really new advances that tend to be on the least traveled road.

**ABOUT TONY TETHER**

1969  Graduated with a PhD from Stanford University and helped start Systems Control Inc.

1978  Systems Control grew to 400 employees and was sold to BP

1978–82  Served as director of national intelligence for the Office of the Secretary of Defense

1982–86  Joined DARPA as director of Strategic Technology Office

1986-92  Became vice president for technology and advanced development at Ford Aerospace

1992–01  Became a consultant and “rent-a-CEO” at times, and returned to government

2001–09  Became director of DARPA

2009  Member of several advisory and corporate boards

    Restarted the Sequoia Group

---
His arrival at Mason coincided with a new project started by the National Institute of Standards and Technology (NIST) devoted to the selection of a new standard in the area of data encryption called Advanced Encryption Standard (AES). Unlike any previous standardization efforts in the United States or abroad, which were often secretly (or openly) controlled by the National Security Agency or its equivalents in other countries, AES was selected through an open competition.

The competition was much like the U.S. Open, except that the participants were not humans but ciphers, developed by multiple groups from all over the world. Through a grueling multi-round competition, these ciphers were evaluated in terms of security, speed in software, speed and cost in hardware, flexibility, simplicity, and lack of any licensing encumbrances. In the final round of the AES contest, it became quite clear that all remaining candidates were sufficiently strong. As a result, their performance in hardware (i.e., when implemented using a specialized chip) became the tiebreaker. This is where Gaj and his first graduate student jumped in, providing the best implementations of all finalists using special reconfigurable chips called Field Programmable Gate Arrays (FPGAs). As a result, one of the two most efficient ciphers—Rijndael, originating from Belgium—became the winner of the competition, and then the current U.S. and a de facto world-wide encryption standard.

In subsequent years, Gaj and his colleague Jens-Peter Kaps formed the Cryptographic Engineering Research Group (CERG). With about 10 PhD students and several master’s students working on their theses and research projects, it is one of the largest and most widely recognized applied-cryptography groups in the United States. In 2010, the group was awarded a highly competitive NIST grant for its research supporting the second major cryptographic contest called SHA-3. The project was a joint work with Virginia Tech and the University of Illinois at Chicago.

The SHA-3 competition was used to develop a standard for cryptographic hash functions. Similar to the case of the AES competition, the Mason team jumped in when about two-thirds of the contestants had been already eliminated due to their security pitfalls. The project required the implementation of more than a dozen candidates in hardware, many of them using multiple variants and hardware architectures.

On the way, Gaj and his team developed ATHENA, an award-winning tool for fair evaluation of digital circuits, through their automated and comprehensive optimization when implemented in FPGAs. The effort paid off in 2012 when a hash function most efficient in hardware, Keccak, was selected as a winner of the competition and the future SHA-3 standard, and the ATHENA Team, was recognized by NIST as one of the primary contributors to the evaluation process.

Fast forward to 2016, and you will find Gaj and CERG heavily involved in two new cryptographic competitions—CAESAR and Post-Quantum Cryptography (PQC). CAESAR is devoted to authenticated ciphers—transformations that combine features of traditional ciphers such as AES,
and hash functions such as SHA-3. Since the number of candidates in the CAESAR contest was the largest in the history of all crypto competitions (57), Gaj and his PhD student Ekawat Homsirikamol proposed and successfully implemented a new strategy for efficient evaluation. They employed high-level synthesis tools, which convert a traditional computer program written in C or C++, automatically into hardware. The result was the same ranking of candidates, but with an effort and development time reduced by about an order of magnitude.

The most recent competition, formally announced by NIST in December 2016, concerns a new class of ciphers and digital signature schemes that are resistant against quantum computers. Predicted in the 1980s and conceived in the 1990s, quantum computers may one day wipe out the majority of modern cryptography as we know it. As a result, researchers are working to find a suitable replacement now.

Taking into account how inefficient any known replacements have traditionally been, the implementation of PQC candidates in hardware (or using a mixture of hardware and software) is a must. Once again, the automated generation of hardware using high-level synthesis tools may appear to be an indispensable tool when trying to either implement or break a large number of investigated candidates.

Gaj enjoys traveling. His conference trips have taken him to every continent except Africa and Antarctica, including his favorite cities of Sydney, Rio de Janeiro, Paris, Prague, Tokyo, Seoul, and San Francisco. He is currently working on a book summarizing his experiences from all major cryptographic contests, from AES to PQC.
Computer Forensics Program and Its Partners Host Cyber Academy

BY BOB OSGOOD, DIRECTOR, COMPUTER FORENSICS

July is known for baseball, soccer, trips to the beach, and now the Computer Forensics Program-led Cyber Academy. For an entire week, rising high school juniors and seniors were exposed to what it would be like to be on the front lines of cyber defense.

The event, hosted at ManTech’s training facility in Herndon, Virginia, started with three days of intensive education. Instructors Bob Osgood, Tahir Khan, Janice Rosado, Sam Blackburn, Simeon Youngblood, and Phil Waterbury led the students through Mason-prepared digital analysis topics, such as network traffic, digital media, and unknown code.

The students spent these three days entirely on the keyboard learning their craft. They had the opportunity to dissect a network traffic capture file looking for evidence of an intrusion, examine digital media for hidden bank account and user access information, and dismember executable code with static and dynamic analysis techniques, safely identifying code artifacts with the goal of determining the true purpose of the code.

The fourth day of the academy was spent at both MITRE Labs and the Department of Homeland Security’s National Cybersecurity and Integration Center where students got to see actual cyber defense in action. The pièce de résistance was a capture the flag event on the fifth day hosted by Kaspersky Lab where students plied their newly minted skills on an actual cyber intrusion.

By exposing high school students to actual cyber skills and having them apply those skills in a real-life setting, we are opening up the world of cyber defense, science technology engineering, and mathematics to them, showing how exciting this type of work can be. All of the skills can be obtained here at Mason’s Volgenau School of Engineering.

Our goal is to make this an annual event.

Partners in this event included Infragard, FBI, Probity-Truxton, Hogan Lovells, and TCecure.
Classroom Role-Playing Gets Students on Their Feet

BY PELIN KURTAY, ASSOCIATE CHAIR

I have a group of close to 100 students in my introductory electrical and computer engineering (ECE) class each semester. Most are declared majors in the ECE program, but roughly one-third of the class comes from the undeclared population in the school. The goal of my lectures is to not only provide them with the technical foundation they need to be successful further along in the program, but also to keep them fully engaged and excited about engineering and ultimately convince them that ECE is fun. Among a number of tactics in my teaching toolbox is the effective tool of role playing.

Now you may think "What does role playing have to do with learning about electrical/computer engineering concepts?" Let me explain the idea with a couple of the examples I have used in previous lectures.

One instance where I employ theatrics is when teaching about single parity checking used for error control in data communication systems. I select a random group of male and female students and assign males to be "0s" and females to be "1s." I ask them to randomly align themselves one after the other to form a "bit stream." The audience is directed to count the number of female students in the stream and a final male or female student is aligned at the end of the group to act as the parity bit, depending on whether we have chosen to work with odd or even parity checking.

The group then marches outside the classroom. Outside, I have one male or female student waiting on standby. One student whose gender is opposite to the standby student is then taken out of the bit stream and the standby is inserted, thereby creating an "error." The modified bit stream then marches back into the classroom and the audience has to identify whether or not an error occurred during transmission by counting the female students in the stream. The fact that an error has indeed occurred is usually identified pretty quickly.

Another example is when teaching about the positive edge triggered D-type flip-flop. One student is assigned to be a drum beater, corresponding to a clock signal. Each beating of the drum translates into the clock transitioning from low to high. Then I select four other students: one to be the D input, one to be the Q output, and the other two to take on the role of the set and clear/reset inputs. The D input is informed that this role does not have much power and that he/she will need to be ultimately overridden by the set or reset input whenever these inputs choose to be active. Then I ask the D input to either raise his/her arms above the head or leave them at the sides in whatever pattern he/she chooses. The students are told that these two arm positions correspond to a logical high or logical low level.

The Q input has to then look at the D input whenever the drum beats and raise his/her hand or keep it down, emulating whatever D is doing at that time the drum is beating. The set and reset inputs are asked to intervene appropriately and override the D input. The Q output has to act accordingly. If the Q output does not know what to do, the students can intervene and provide input on the correct arm position.

As a fan of the performing arts, I am always trying to come up with ways to keep the materials interesting. I feel that this approach of role-playing takes the pedagogy of active and collaborative learning in the engineering classroom to a whole new level.
Adopt a ‘Bot

Small but mighty, the ECE ‘bot, Edith, helps students combine the disciplines of electrical and computer engineering. Named after the first woman electrical engineer, Edith Clarke, she is a true collaborator who works across curriculum boundaries to make this a fun, hands-on learning experience for all our students.

Please support the ECE Department in continuing its cutting-edge research and help ECE students by adopting Edith.

Go to Volgenau.gmu.edu/give/adopt-a-bot and make a donation today.