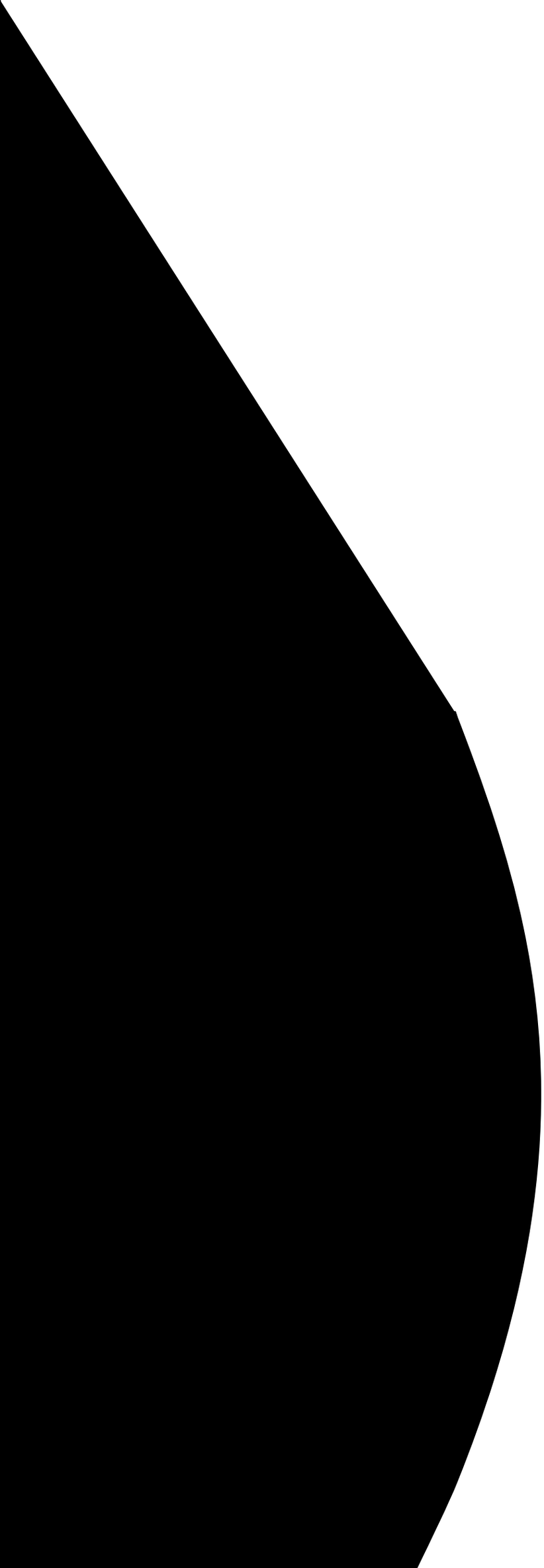
UNIVERSITY OF CALIFORNIA, SAN DIEGO

In recent years the National Academy of Engineering (NAE) conducted an in tense study of grand challenges and opportunities in engineering facing those



De ning the Semiconductor Roadmap

The Computer Science and Engineering department now boasts seven active faculty members who are Fellows of the Institute of Electrical and Electronics Engineers (IEEE).

In 2010 Andrew Kahng joined their ranks. IEEE cited his contributions to “the design for manu facturability of integrated circuits, and the technology roadmap of semiconductors.” Indeed, the UC San Diego computer science alumnus (Ph.D. ’89, M.S. ‘86) has for the past 15 years played a pivotal role in the development of the International Technology Roadmap for Semiconduc tors (ITRS), primarily guiding its work to predict future system drivers and design technology requirements. Kahng has also served on the editorial boards of IEEE Transactions on VLSI, IEEE Transactions on Circuits and Systems I, and IEEE Design and Test (where he contributes “The Road Ahead,” a regular column focused on underlying technologies and future developments in the design and test of integrated circuits).

Kahng joined Dean Tullsen (2009), Rajesh Gupta (2004), Jeanne Ferrante (2005), Bill Howden (2001), C.K. Cheng (2000) and Walter Burkhard (2000) as IEEE Fellows. Former CSE faculty elected IEEE Fellows include Larry C (-)Tj E0ra2000) an0 AndreChilsen (27tsas IEE hin ths worgul Seed

Many energy e ciency gains worldwide have been due to computer sci ence and engineering technology. So it should come as no surprise that CSE and ECE Prof. Andrew Kahng sees another power revolution ahead – thanks to processors designed to permit more processing with less energy. As a leader in the global e ort to create a roadmap for the future of both semi conductor technology and its market drivers, the computer engineering professor is involved with a number of research projects that are rethinking the way processors are designed to enable higher performance using less power.

Kahng's group takes a broad view of energy issues as they relate to-semi conductor scaling, density (more functions per chip), device performance, and the leakage of increasingly expensive energy as scaling continues.

The 'power management gap' (pictured at right) will have increased 100

CSE Research Scientist Yuvraj Agarwal received UCSD's Outstanding Faculty Award for Sustainability for 2012 – fitting recognition for a series of research projects and novel solutions that are helping to make offices and buildings more energy efficient. One example: the UC San Diego Energy Dashboard, a Web portal that allows anyone to track how much power is being used by any building on the UC San Diego campus (and even floor by floor in the CSE Building).

Since then, Agarwal and Ph.D. student Thomas Weng have published a groundbreaking paper in the journal IEEE Design and Test Special Issue on Green Buidings on the use of sensing and actuation to improve energy efficiency.

The researchers used CSE's headquarters building as a stand-in for mixed-use commercial buildings, which account for roughly 35 percent of total electricity consumed in the U.S. each year. "Even a small improvement in energy efficiency could translate into substantial savings here and around

Each time you connect to a secure Web site (say a bank's site), you begin by downloading a certi cate published by the site, which asserts that its Web address is legitimate and contains a public key that your computer can use to establish a secure connection. The public key, ostensibly, prevents anyone else from spying on your connection.

But according to a paper presented at the 21st USENIX Security Symposium in August 2012, vulnerable public keys are "surprisingly widespread" on the Internet, especially for certain types of devices such as routers and rewalls. The paper, "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices," won the confer ence's Best Paper award.

UC San Diego postdoctoral re searcher Nadia Heninger co-authored the paper with three colleagues from the University of Michigan: Zakir Durumeric, Eric Wustrow and J. Alex Halderman. To pursue their research, Heninger and her colleagues scanned the entire Internet in 24 hours and col lected public keys from 22 million hosts, which werd dr .06erd dr mo8]TJ ug /Span <</M07 8n <</675 BDC iH673 >>BDC 0 Tw 0 - devsts, which wed t4310(our c)6(onnec)-14(a routers and de4Cgenew 0 -

With the explosive growth in con dential data housed in 'the cloud,' where it may seem more vulnerable than if it were located on a local hard drive, security experts are looking to cryptographers for help.

"Imagine running your most computationally intensive programs on your large data sets on a cluster of remote computers, and in a cloud computing environment, while keeping your programs, data, and results encrypted and con dential," wrote CSE Prof. Daniele Micciancio in a 2010 article in Communications of the ACM.

The idea of such fully homomorphic encryption traces back to the earliest public-key encryption schemes in the 1970s, but it wasn't until 2009 that IBM's Craig Gentry proposed a new approach to constructing fully homomorphic cryptographic systems. "Now, most cryptographers (me among them) are convinced the Holy Grail exists," said Micciancio. "In fact, there must be several of them, more or less- ef cient ones, all out there waiting to be discovered."

Gentry's work was the rst real breakthrough in using lattices to reach that Holy Grail. "Since then, a dozen other schemes have been published, and all are based on lattices," explains Micciancio, a theoretical computer scientist. "So from what we can tell, lattices are the only way to build homomorphic encryption, perhaps because lattices can mathematically support both addition and multiplication, so you can perform just about any operation."

Lattices have been used historically in math and coding theory, and many applications in computer science date back to the early 1980s. "They were even used in cryptoanalysis to break codes," notes Micciancio. "But it wasn't until the late 1990s that we started to nd ways to use lattices to build secure cryptographic systems."

For his part, Micciancio set about proving the hardness of lattice-based codes – to prove that they couldn't be broken. "These days cryptography and security are everywhere on the Internet and you cannot wait a few years to see if a function works or not," he explains. "There is a strong theoretical basis and evidence that these functions are hard to break."

Reaching the Holy Grail, however, requires much greater e ciency in lattice cryptography in order to make it run faster while taking up less space. "My work is at the foundation of lattice cryptography," explains Micciancio. "Most of this foundational work will stay fresh for a long time. My current work is focused on trying to move lattice cryptography from theory to something that is e cient enough to be usable in practice, and that requires not just an engineering e ort, not just implementation, but also the math that needs to be developed to achieve its maximum potential e ciency."

To that end, Micciancio delivered a paper on the use of 'trapdoors' with lattices at the April 2012 Eurocrypt conference in Cambridge, England. Trapdoors have been used in cryptography since the term was coined in the mid-1970s. A trapdoor includes special information without which it would be impossible to do a computation in one direction, even though it is easy to compute in the other direction.

Trapdoors are fundamental building blocks used in many lattice cryptography applications. "The potential applications to securing the cloud are clear

Better Image Searches… Through Birding?

Searching text via Google or Wikipedia is a breeze compared to searching for just the right image on the Web. Now a team led by CSE Prof. Serge Belongie is determined to combine expertise in computer vision with citizen science in order to come up with a unique approach to image search. It's called Visipedia, and the initial proof of concept involves an ambitious plan to build a visually searchable database of over 500 North American bird species, curated by the Cornell Lab of Ornithology.

Computer scientists from UC San Diego, UC Berkeley and Caltech have designed Visipedia as a search syste that can interact with users to provide more accurate results. The ultimate goal is to ll the image gap in the

Sequencing the Dark Matter of Life

Entire species of bacteria have traditionally been o -limits when it comes to DNA sequencing, because they cannot be cultured to provide the roughly one billion identical cells required by standard sequencing methods. This so-called 'dark matter' of life includes the lion's share of bacterial species living on the planet, including microorganisms that could yield new antibiotics and biofuels, and microbes living in the human body. "This part of life was completely inaccessible at the genomic level," says CSE Prof. Pavel Pevzn a pioneer of algorithms for modern DNA sequencing technology.

Now a team of scientists including Pevzner, graduate student Hamidreza Chitsaz, and UCSD Mathematics Prof. Glenn Tesler (a former postdoctoral researcher in CSE), have developed an algorithm that dramatically improves the performance of software used to sequence DNA produced from a single-bac terial cell. The breakthrough allows researchers to assemble virtually complete genomes from DNA extracted from a single bacterial cell. Using the new algorithm to enhance Multiple Displacement Ampli cation (MDA) technology developed a decade ago, scientists can start with just one cell, but capture 90 percent of genes – even for species which could not be se quenced until now.

If that sounds like magic, the new algorithm comes close: the innovation not only makes it possible to sequence the DNA of most bacterial life, but also to do so economically. The ram i cations for human health could be astounding – especial- ly given that bacteria account for roughly 10 percent of the weight of the human body.

As described in the journal Nature Biotechnology

GreenDroid vs. Darmostly passive in order to sta(TJ 0.009 Tw 0 -1.75 TD [( )83(“)-28(W)33(e believ)1
are the pattern of logic gates that are spatially placed

Replacing the Flash in Memory

Today's computers are awash in data. Making sense of that data requires computer systems that can keep up, and one solution is to develop solid-state storage devices that give computers fast, energy-efficient access to the data they need.

Enter CSE's Non-Volatile Systems Laboratory (NVSL), which builds prototype storage systems that integrate cutting-edge memory technologies such as phase-change memory (PCM) and spin-torque transfer memories (STTMs). These prototypes include novel features that work hand-in-hand with specially engineered software components to reduce or eliminate performance bottlenecks left over from the disk-based storage systems of the past. The result is flexible computer systems that can help sift through vast amounts of data quickly and efficiently to support data-intensive applications such as Web search, social networks, and online fraud detection.

PCM and STTM aim to replace the flash memory that currently powers iPads, iPods and cell phones. They are faster and have a simpler interface than flash. They are more reliable as well, and they pave the way for data-processing systems powerful enough to tackle challenging problems, from genome assembly and modeling the earth's climate to analyzing Web content in real time.

"We have found that replacing flash memory and disks will require more than simply swapping one memory technology for another," explains CSE Prof. Steven Swanson, who directs the NVSL. "When PCM and STTM enter the mainstream they will be fast enough to reveal hidden inefficiencies and latent bottlenecks in existing computer systems – systems optimized for disk-based storage systems that were up to 50,000 times slower compared to these emerging memory technologies."

To identify and eliminate these inefficiencies, Swanson and his team built the world's first, publicly-demonstrated PCM storage array, called Onyx*. Next, they used performance data from Onyx (and a related system called Moneta) to redesign the Linux operating system to match the level of performance that Onyx can deliver. In many cases, says Swanson, NVSL had to throw out existing components and start from scratch. In the process, they redefined how Linux provides programs with access to their data and how the system protects data from inadvertent corruption. The result: a 20-times improvement in performance for Moneta and Onyx, and a huge boost in performance at the application level.

"Our version of Linux is ready for these new storage devices, but applications are not," says Swanson. "Databases also suffer from

Giving Computers a Con dence Boost

Sometimes it might seem like computers need humans like sh need bicycles. But the truth is, most computers still need humans—especially when it comes to teaching them the di erence between sh and bicycles.

That's where CSE Prof. Sanjoy Dasgupta's research comes in. Dasgupta and his colleagues are developing techniques to enhance machine learning so that interactions between computers and humans are more e cient, and data mining and classi cation more accurate.

"There's a lot of data out there, so much so that there is no way that humans can process, label and interpret all

In a world where public records can be searched and downloaded with the touch of a keystroke, the cost of physically accessing, recording and tabulating this information has been a de facto barrier to its use and dissemination. The ease of access to everything from grocery-buying habits to patterns of political donations, and the development of powerful tools for the management and analysis of this data, have led computer scientists to explore ways to use such data while

Datacenter Networks

The growth of complex, data-driven Internet applications such as Web search, social networking, interactive maps and streaming video has accelerated at an astounding rate. Today a single such application may harness hundreds of thousands of servers, all working together. Keeping pace with this new workload has required developing a new generation of communications networks designed specifically for the datacenter environment. These networks must deliver sufficient bandwidth to these resource-hungry applications, while ensuring that they are scalable, manageable, flexible, and have low-cost and low-power requirements.

This new domain of datacenter network design is one in which UC San Diego has taken a leadership role, designing and building new network switches that have been highly influential in industry and academia alike.

One of the key challenges in datacenter network design is that while it is possible to grow computing and storage incrementally by simply buying more servers and more disks, growing the network has required increasingly specialized and expensive switches. These traditional, ‘scal495 >>Btally o1 has required r1 Twdevgyequired

Computing systems fail. It's a fact of life. The trick, says CSE Prof. Yuanyuan (YY) Zhou, is to design around system failures so they are easy to diagnose and, ideally, able to be tolerated.

"When we talk about failures, we're talking about when a program crashes, or when the operating system goes to a blue screen, or when Google or Gmail is suddenly not available," explains Zhou. "Google's datacenter, for example, has a system failure every one-to-two seconds on average. The more machines a datacenter has, the more chance there is for things to fail."

It's a problem that affects just about every aspect of the tech industry, from storage system providers to data warehousing and network infrastructure companies.

"Storage failure is a really important issue, because a failure could mean that data is actually lost, not just that it isn't accessible," says Zhou, who co-authored three papers in 2012 on 'proactive' logging, including one delivered at the USENIX Symposium on Operating Systems Design and Implementation in October 2012.* "Their customers include a lot of banks, for example, so losing data is a big deal. And in the case of a network infrastructure company, it's the backbone of the Internet, so when there is a failure, information just isn't being communicated."

The problem with most software companies and service providers is that they design for functionality and performance and focus on what should happen when things go right. When something goes wrong, most companies rely on the end user to send an 'error report' in an attempt to diagnose the failure.

However, many users don't like sending error reports back, because it could compromise their privacy, and sending an error report won't necessarily help the end user with the problem they are currently experiencing. After all, most reports are used to diagnose errors so they can be eliminated from future versions of the software.

futurJ EM65lprror re0 is a b1(t6ging goes w Tw 0c(, ( )83-40(T)3uc) luxuvic)6(and ")]TJ EMC /Span <</MCID 2732 >>B4C 0.094 Tw 44-1.824 TD [(W)16(
ec9(y)1(and soodo send : ANetA)]TJ EMC /Span <</MCID 2732 >>B51 0.094 Tw 4 -1.824 TD [(Ho)7(w Tw 0 -1.m.lE)10(,a ar)1n o 0 is a b(t) eril.lE,chnic
and tonm4(W)17m(, Mot)6(aw18 Tw 0 -1.m.lEMC /S(r)10(( )]TJst)6(r)i<</MC3sm(q8)]TJ EM6GMC /Span u4d6(r)i<</MC3sm(q8)]TJ EM6GMC /S0 s

With funding from NSF as well as Intel, Cisco Systems, NetApp, Motorola, IBM

As Joseph Stalin infamously said, “I consider it completely unimportant who in the party will vote, or how; but what is extraordinarily important is this — who will count the votes, and how.” The Digital Age-version of that statement revolves around the multiplicity of computerized systems used in capturing, reporting and tabulating votes. Indeed, as our democratic process has come to depend on a trusted tier of hardware and software, the security concerns of these systems have become ever more important. CSE Prof. Hovav Shacham has been one of the researchers leading this examination.

Shortly after joining UC San Diego in 2007, Shacham was part of the team commissioned by then-California Secretary of State Debra Bowen to complete a top-to-bottom review of the state’s electronic voting systems. With colleagues from Stanford, Rice and the private sector, Shacham analyzed the source code for the widely-used Hart InterCivic system. He identified a range of vulnerabilities that could potentially allow votes to be manipulated, and the secrecy of a citizen’s vote to be

Traditionally, computer security has been viewed as a problem of technical origins.

CSE's 'Broad and Deep Curriculum'

The Computer Science and Engineering department prepares its undergraduate students for top placement in a competitive, high-tech job market, and for advanced studies in graduate school. From processing images and sounds in the introductory computer science course as a freshman (CSE 8A), programming robots and smartphones as a sophomore (CSE 87), rendering photorealistic images using computer graphics as a junior (CSE 168), to designing and implementing

DRIVING INNOVATION

The California Institute for Telecommunications and Information Technology (Calit2) is a large, multi-disciplina /Span 0V1eepareci0(nstitut)6(locdua)4(t)6d neetn th2(CSbuild(ti)1510(.Di

IN THEIR OWN WORDS

Richard C. Ord

Boris Babenko is relatively fresh from earning his Ph.D., and he has already built and sold his rst company, Anchovi Labs, to Dropbox.

Babenko earned his B.S., M.S. and Ph.D. degrees in Computer Science and En gineering at UC San Diego, the latter in the eld of computer vision, under advisor Serge Belongie. “Boris has a remarkable, world-class combination of

Thomas Ristenpart (Ph.D. ‘10) works at the interface between systems and cryptography, two foundations for making systems and services secure in an online world where attacks are the norm. His dissertation work introduced new ways to design and analyze cryptographic hash functions, and developed format-preserving encryption techniques for legacy databases that enable services to encrypt data originally stored in plain text. Ristenpart’s work also addressed security and privacy risks in emerging technologies, such as information leakage in public cloud-computing systems, and

There aren't very many computer scientists with a section of their CV about "Ships I have been on," but then again, CSE alumnus Kevin Fall (Ph.D., '94) has had a relatively unconventional career.

One of the ships cited on his resume, the U.S. Coast Guard Cutter Healy, is the most

It may not seem so unusual in a company created by twentysomethings to change the 21st century world, but Taner Halicioglu was already a veteran of several high-pro le startups by the time he joined Facebook in 2004.

The company was so new that he was, he recalls, Facebook's rst 'real' employee (after the company's founders).

Halicioglu, who moved back to the Bay Area after graduating from UC San Diego with a B.S. in Computer Science (Revelle College, Class of '96), helped transform Facebook into the ubiquitous social network it quickly became. As the company's rst operations honcho on the pro duction side, Halicioglu was respon sible for building out the initial hard ware infrastructure, and he helped scale Facebook over 2,000-fold in the ensuing ve years.

Facebook, however, isn't the only mega-hit on Halicioglu's resume. Pri- or to joining Facebook, he worked for nearly three years at the similarly iconic eBay (2002-04). There he built monitoring tools for eBay's Network Operations Center. The tools, many of which are still in use today, al- lowed eBay to keep close tabs on the performance of its databases, Web servers and applications servers, all of which were at the heart of the company's success.

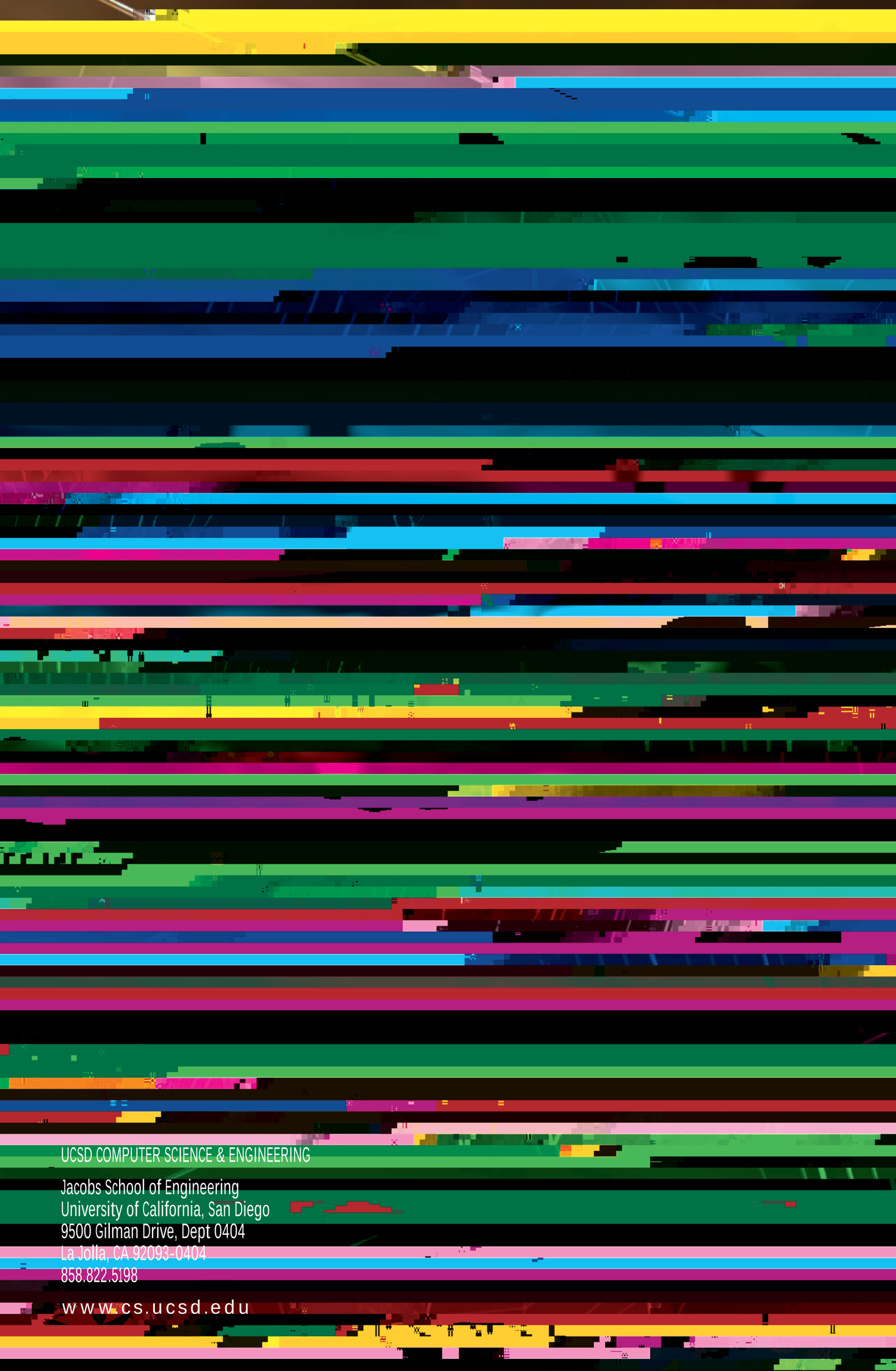
After graduating in 1996, Halicioglu spent three years at a company that, through a series of buyouts, became another hot property of the 1990s technology boom: Global Crossing. He then worked for a startup called Loudcloud (now part of HP), where he built automated tools for DNS control by systems administrators, until he joined eBay.

After his ve-year run at Facebook, Halicioglu left the company to work in the Irvine headquarters of Blizzard Entertainment. He was the lead reliability engineer for its Battle.net online gaming platform, which sup ports millions of members worldwide who play epic, multiplayer fanta- sy games, including World of WarCraft, StarCraft II, and Diablo III.

Since leaving Blizzard in late 2011, Halicioglu has focused on investing. On his own Facebook page, the UCSD alum brie y recorded a 'life event' in his pro le on May 18, 2012 – the day Facebook went public on the Nasdaq Stock Exchange.

Halicioglu considers himself "a computer geek, car geek, music geek, and geek geek." He has composed and played music using MIDI synthe sizers since high school in Palo Alto, Calif., not far from where he worked at Facebook. Music was also important to Halicioglu at UCSD, where his area of focus was music technology.

In his nal quarter at UCSD, Halicioglu was a teaching assistant for the



UCSD COMPUTER SCIENCE & ENGINEERING

Jacobs School of Engineering
University of California, San Diego
9500 Gilman Drive, Dept 0404
La Jolla, CA 92093-0404
858.822.5198

www.cs.ucsd.edu