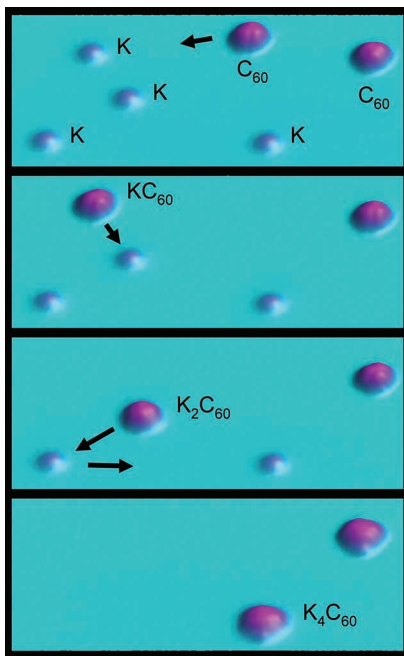


# The New Dope on Semiconductor Doping

**A** University of California, Berkeley, researcher has developed a way to apply semiconductor dopants at the atomic level. Controlling the amount of dopant applied is increasingly important as the size of wires, diodes, transistors, switches, and other semiconductor elements approaches molecular scale.

During semiconductor fabrication,



*These photos show how a UC Berkeley researcher's new technique enables carbon molecules to absorb potassium atoms as dopants. In the past, chip makers frequently added dopants, which improve a material's performance by changing its electrical properties, in bulk because their exact quantity or placement wasn't important. As semiconductor elements get smaller, being able to add tiny amounts of dopants in a controlled manner becomes critical.*

manufacturers typically add dopants to semiconductor materials, such as silicon, to change their performance by altering their electrical properties. P-type doping adds elements such as boron or indium to remove electrons. N-type doping inserts elements such as arsenic, phosphorous, or potassium to add electrons.

Currently, chip makers frequently add dopants in bulk to semiconductor materials. However, as the elements become smaller, the amount and placement of doping must become more precise. "If you make your electrical components small enough, the presence or absence [or placement] of a single dopant atom influences the properties of the devices," said Michael F. Crommie, professor of physics at UC Berkeley.

In response, Crommie developed a technique for attaching dopant atoms, one at a time, to individual molecules, permitting the tight control and fine tuning of their electronic properties. Conventional tools have not offered such precise control.

Crommie and his group used the probe of a scanning tunneling microscope—whose sharp metal needle reads a surface when voltage is applied—to move large buckminsterfullerene carbon molecules across very cold, highly

polished silver crystal toward potassium dopant atoms. When a molecule gets close enough, it sucks up an atom.

Crommie conducted his experiment in a vacuum chamber at 7 degrees Kelvin (-266 degrees Celsius), which is close to absolute zero. The extreme cold is critical because it keeps the atoms from moving around, which makes it easier for the molecules to absorb them.

Using extreme cold would not necessarily be practical or cost-effective for semiconductor manufacturing. On the other hand, it wouldn't necessarily be required for all dopants or semiconductor materials.

Crommie said the purpose of his work was not to make devices but to conduct basic research on fundamental molecular behavior. "We hope to eventually create devices at a molecular scale, but if we want to create new devices, we need to understand small molecular structures."

"There is a great deal of interest with no practical applications as of yet," said Jun Nogami, University of Toronto professor of materials science and engineering.

It could be years before practical devices are made commercially using this technology, Nogami noted. ■

—Linda Dailey Paulson

## PARC Develops Software to Connect Devices

**P**alo Alto Research Center scientists have created a technology that promises to let consumer-electronics devices communicate with one another and access content and

resources across hardware, software, and networking platforms.

PARC's interoperability technology, Objé, is designed to make it easier to use a single device to access many dif-

ferent types of content and resources. And the software would help providers save money by letting them design just one version of their content for multiple platforms.

Industry observers say this could increase the adoption of digital media and the devices that play it. Adoption has been slower than hoped for, largely because of compatibility issues.

The Obje software architecture establishes a common means of communication to provide interoperability across platforms, said Hermann Calabria, PARC's principal of business development.

In a sending device, Obje recognizes the capabilities that the receiving device needs to work with code that it is transmitting, such as a codec to work with MPEG files. It also recognizes which of those capabilities the receiving device lacks. Obje then sends the recipient the code that will provide the missing capabilities. An older machine that can't work with Obje can work via a proxy device.

With Java-enabled devices, Obje can use a Java virtual machine, rather than send missing code, to achieve device, OS, and network neutrality. A JVM interprets compiled Java binary code so that a processor can perform a program's instructions. Any Java program can run on a platform for which a JVM has been designed, thereby enabling platform interoperability. Calabria noted that Obje could also work with cross-platform approaches other than Java.

The technology need not be pre-loaded on every networked machine to work, as long as machines can connect to an Obje-enabled device—such as a set-top box or stereo receiver—that could serve as a hub.

Researchers hope to make Obje usable on handheld devices. So far, they have shown that the software will run on resource-constrained devices by testing it on a Hewlett-Packard iPaq PDA. They are planning more tests, although Obje currently is too expensive and requires too much memory

and processing power for handheld devices.

Even if Obje proves to be technically successful, the technology's marketplace success will still depend on industrywide adoption and promotion. PARC sources say they have spoken with several companies, which they declined to name, about turning Obje into a commercial project.

Home-entertainment networking, which Obje would facilitate, is a hot topic because of its enormous profit potential for device makers and content providers.

Until now, said Vamsi Sistla, director

of broadband and residential entertainment technologies for ABI Research, a market analysis firm, "No one technology or standard or protocol has been able to address the many networking and technological challenges. There are already more than 60 or so standards and protocols."

To address compatibility issues, companies have formed and joined industry groups such as the Digital Home Working Group ([www.dhwg.org/home](http://www.dhwg.org/home)) and the UPnP (universal plug and play) Forum ([www.upnp.org](http://www.upnp.org)). ■

—Linda Dailey Paulson

## Creating Blazing Hot Images of Fire

When moviemakers need to show fire, they traditionally use the real thing because animations typically haven't had the kind of detail that makes the images effective. However, using real fire can create safety hazards and limit the size of the blazes that can be shown.

Now, though, Stanford University assistant professor Ron Fedkiw; University of California, San Diego, assistant professor Henrik Jensen; and former Stanford postdoctoral student Duc Nguyen have developed software to create realistic fire animations, overcoming shortcomings that have kept moviemakers from using such applications in the past.

Previously, generating realistic computer simulations of fire was difficult because it required a great deal of detail, Fedkiw explained.

With the new software, users can set initial conditions for the fire, such as temperature, type of fuel, and surface shape. Taking advantage of today's powerful computers with large amounts of memory, the technology solves equations that describe swirling fluids, expanding gases, and vaporized fuel, then it renders images such as smoke, soot, and igniting objects.

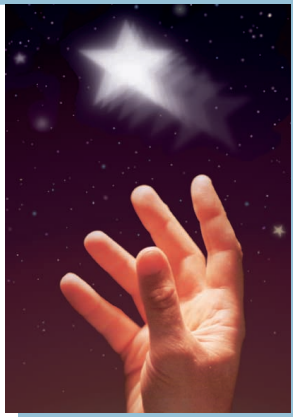
The software uses this information to create animated flames in much the same way that fire actually occurs. The technology has elements combust at different times, in different patterns, and in different colors depending on the heat level, and it creates images of black soot and smoke as they cool over time, as would happen in a real blaze. The software also adds many fine details, such as eddies in swirling smoke, to make the images more effective.

The technology takes about five minutes to generate a frame of animated fire, Fedkiw explained, which is comparable to the time it takes to render many photorealistic animations such as those of hair and water.

He said enabling greater and easier control of fire animations could require another year or two.

Filmmakers and special-effects companies have expressed interest in the fire-animation software, according to Fedkiw. The technology could also be used for applications such as virtual reality training for firefighters. ■

—Linda Dailey Paulson



## REACH HIGHER

Advancing in the IEEE Computer Society can elevate your standing in the profession.

Application to Senior-grade membership recognizes

- ✓ ten years or more of professional expertise

Nomination to Fellow-grade membership recognizes

- ✓ exemplary accomplishments in computer engineering

GIVE YOUR CAREER A BOOST

UPGRADE YOUR MEMBERSHIP

[www.computer.org/join/grades.htm](http://www.computer.org/join/grades.htm)

# System Uses Existing Attacks to Predict Future Threats

**A** US company has developed a technology for analyzing current computer intrusions and extrapolating them to determine how future assaults might look, even before hackers develop them.

The ability of Icosystem's technology to identify at least some new types of attacks could overcome the limitations of many firewalls, antivirus programs, and other security applications that recognize only the code signatures or attack patterns of known assaults.

Eric Bonabeau, Icosystem's chair and chief scientific officer, said that while predicting new attacks would be a beneficial side effect, his technology's main goal is to discover systems' security vulnerabilities.

Today's security systems typically analyze traffic for signs of past malicious activity, such as specific code strings or data arriving at an unusual TCP/IP input port. Icosystem's technology takes information from known intrusion and virus approaches, sometimes found in online hacking soft-

ware, and uses artificial evolution to show how the attack scripts might morph.

The system systematically changes the scripts to find the most deadly mutations. The Icosystem technology also combines parts of hacker programs to see how new attacks would evolve.

The security software could then implement predesigned defenses for vulnerabilities to these most likely assaults or recognize the signs of hackers launching these attacks, via code strings, entry ports, or other signatures.

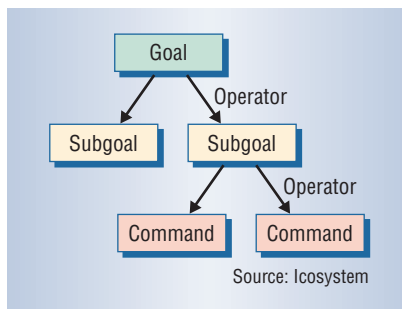
The US Army's Computer Crime Investigation Unit sponsored the experimental phase of the technology, which is still in the prototype stage. "There are lots of details to be worked out," Bonabeau explained.

Some industry observers say the approach could lead to a smarter generation of intrusion-detection systems. But Eric Ogren, senior analyst for the Yankee Group, a market research firm, expressed skepticism.

Ogren said Icosystem's technology might be a good system-auditing tool to identify vulnerabilities but would be minimally effective as a safety tool because it would only detect, not prevent, attacks. Also, Icosystem's technique wouldn't help with new attacks that aren't based on old approaches.

Bonabeau said Icosystem may never release a commercial version of the system because it might require more work and staff expertise than companies have available for such purposes. ■

—Linda Dailey Paulson



*Icosystem has developed a technology for analyzing computer intrusions and extrapolating them to determine how future attacks might look. The system does this in part by abstracting a hacker's goals from the commands actually used in an attack, via subgoals in between, and then generating scripts of potential new assaults based on the initial incident.*

Editor: Lee Garber, *Computer*,  
l.garber@computer.org