

New Mobile Device Screen Saves Energy

A US company has developed a new technology that would drastically reduce power usage by mobile devices' displays. The iMoD (interferometric modulator) approach would enable cellular phones, MP3 players, and other battery-operated, power-constrained devices to run all day in many cases.

This is particularly important now because consumers are demanding more from their mobile devices, such as the ability to stay on all the time, explained Greg Heinzinger, president of iMoD developer Qualcomm MEMS Technologies.

"Current [liquid-crystal] displays are not up to the challenge," he said.

Most portable devices work with transmissive LCDs, which use polarizers and filters to block light and remove the wavelengths of a bright white light source to create various

colors. The liquid crystals modulate the light's intensity.

A backlight makes the overall display brighter or darker as needed, depending on the ambient light. Because the filters and liquid crystals block so much of its output, the backlight must be powerful—and use considerable energy—to provide the required brightness. Thus LCD displays consume considerable power and are a major drain on mobile devices' batteries, noted Heinzinger.

iMoD uses optical interference to display images. Pixels in an iMoD display consist of a flexible thin-film mirror located a few hundred nanometers from a transparent glass substrate. "When ambient light enters this cavity and reflects off the thin-film mirror, it interferes with itself, producing a resonant color determined by the height of the

cavity," Heinzinger explained. The system produces different colors by varying the distance between the mirror and the substrate.

Applying an electrical field to the cavity provides additional reflective and absorptive properties. In dim or dark conditions, an integrated front light illuminates the screen, Heinzinger said. Because the front light is reflected through the system by the mirror and because it is not filtered or otherwise blocked, it can be less powerful and consume less power than LCD backlights.

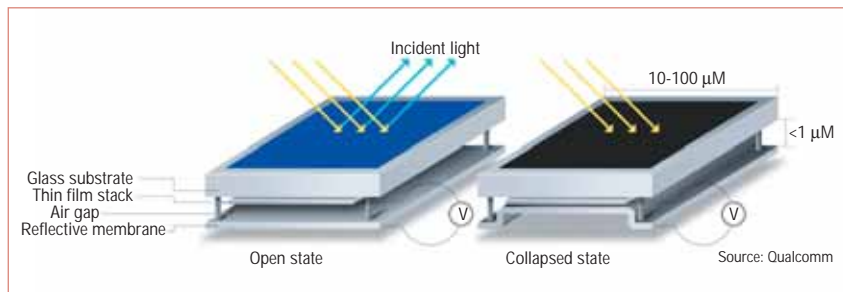
The first prototype iMoD screens will show images only in black and gold, which will be sufficient for text-based and several other types of applications. However, Heinzinger added, Qualcomm has already demonstrated the ability to use the technology to produce full-color images.

"From what little I've seen of them, they look fairly good for a reflective display," stated Steve Jurichich, director of display technologies for DisplaySearch, a market research firm.

However, he said, like other reflective displays, iMoD offers low contrast in dark environments. Jurichich said he also hasn't seen how well iMoD technology handles video.

Qualcomm has not announced when it plans to release iMoD commercially.

Companies such as E Ink, Kent Displays, Nemoptic, and SiPix Imaging are also working on low-power mobile-device screens. ■



Qualcomm has developed a technology that would reduce power usage by mobile devices' displays. In the iMoD approach, a pixel consists of a glass substrate located just above a reflective conductive membrane. When users apply a voltage to the membrane and the glass, the membrane is drawn toward the glass by electrostatic attraction. If they meet, the pixel appears black. The application of lower voltage separates the two. When ambient light enters the gap and reflects off the membrane, the light rays interfere with one another, producing a resonant color,

News Briefs written by **Linda Dailey Paulson**, a freelance technology writer based in Ventura, California. Contact her at ldpaulson@yahoo.com.

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

Queen Bots Pose Security Threat

Malicious bots, which hackers send to vulnerable computers and then use to launch attacks, have just gotten more dangerous. Hackers are now using *queen bots*, in which the executable file containing the malicious code is packed.

Before sending malware to a victim, hackers use *packing* to hide the executable that launches the desired attack. The technique adds a code string to make it harder for antivirus programs to recognize the file as malware. Once on a victim's computer, an executable file unpacks and launches the malware.

Hundreds of packing programs are readily available online for sharing by attackers and malware writers, said Oliver Friedrichs, director of security vendor Symantec's Security Response Center.

Hackers often repack and redeploy bots that have been packed and used previously, he noted. They also frequently use multiple packers, encryption, and other approaches to further obfuscate the code.

By obfuscating the malicious executable's original code signature, packing keeps antivirus software from recognizing the malware and leaves users vulnerable to bots, which frequently launch spam, phishing, or denial-of-service attacks. When the victim's computer executes the malware, it turns the machine into one of many *zombies* that subsequently launch the intended attacks upon receiving the hacker's command.

Antivirus applications typically recognize malware by their code signatures, which are stored in the product's database. Changing the signatures makes them more difficult to detect.

Hackers can change existing queen bots remotely. So far, though, noted Friedrichs, none of the bots he has seen are *polymorphic* and thus can't change their code signatures on their own.

Security experts are fighting back against queen bots, so named because, like queen ants, they exercise centralized control over a system and rapidly produce offspring, noted Georgia Institute of Technology doctoral candidate David Dagon, who has studied the technique.

According to Friedrichs, Symantec has examined code strings common to packers and developed signatures to identify queen bots in both packed and unpacked forms. The company has developed technology that creates new unpackers, distributes them to customers, opens infected files, and neutralizes the malicious code before the bots get onto a user's system.

Sophisticated packing programs are a bigger challenge because they make more complex and irregular changes to code.

Dagon and veteran Internet researcher Paul Vixie have created a

public malware repository (<http://malfease.oarci.net>), currently in beta form, to deal with queen bots and other forms of automated malware creation and updating.

The site allows visitors to submit samples of such malware. Registered industry and academic researchers can analyze and otherwise work with the unpacked versions of samples, explained Dagon.

A number of organizations, including some antivirus vendors, have already contributed to the repository. According to Johannes Ullrich, chief research officer of the SANS Institute, his information security research and training group will typically send unusual malware samples.

Dagon said he wants more antivirus vendors to take part, but noted that the industry's competitiveness may limit participation. ■

Building Fantasy Worlds Virtually

An increasing number of companies and organizations are incorporating customized, complex online virtual worlds, to promote their businesses, train employees, conduct research, or accomplish other goals.

This has spurred a growing market for individuals and technology companies—such as Advantar, Electric Sheep, and Rivers Run Red—that build these virtual worlds.

Previously, virtual worlds were generally built by online gaming providers. Otherwise, only companies with trained personnel could design and construct their own environments using specialized design tools.

But now, many more companies can hire designers with their own toolsets to build virtual environments for them. For example, customers can work with designers who use tools from Linden Lab to build virtual communities within its Second Life 3D virtual world (<http://secondlife.com>).

Virtual worlds can be used for numerous purposes, such as entertainment—as in games or fantasy theme parks—or corporate activities—as in virtual conference or training centers.

Electric Sheep CEO T. Sibley Verbeck noted that his company generally charges from \$10,000 for small virtual worlds to \$1 million for elaborate environments, such as a recent virtual resort that the Starwood Hotel chain will use to research future construction of an actual vacation complex.

He said organizations are willing to pay companies to do this work because they don't have and can't use the complex tools necessary to build virtual worlds.

In addition, some designers let customers own the intellectual property behind their virtual worlds, which makes the approach more attractive.

IBM Stores Data in a Single Molecule

IBM researchers have developed a single-molecule device that can store and retrieve data. This could help increase storage capacities, at a time when silicon-based technologies may be approaching their limits, and could become a key development in molecular computing.

The scientists at IBM's Zurich Research Laboratory worked with the bipyridyl dinitro-dithiol molecule—about 2 nanometers long and with 1/1,000,000th the volume of current transistors—that Rice University professor James Tour designed.

BPDN-DT, previously used in single-molecule transistors, is made of carbon, hydrogen, nitrogen, oxygen, and sulfur. It is in a class of compounds—known as Tour wires in

honor of the Rice professor—frequently used in molecular electronics because of their electrophilic qualities.

The experiment mounted the BPDN-DT molecule between two gold electrodes and applied an electric current, said IBM research staff member Heike Riel.

This caused the voltage flow within the molecule to change, in essence causing the molecule to switch states. This creates the ones and zeros of stored binary data. Each molecule could store one bit.

Riel said she and other researchers are trying to determine the exact mechanism that causes the molecule to switch states.

Testing was primarily conducted in cold conditions because the gold atoms on the surface of the electrodes are very mobile at room temperature—22 degrees Centigrade—and thus won't reliably cause the BPDN-DT molecule to switch states.

The maximum rate at which molecules could change states—which

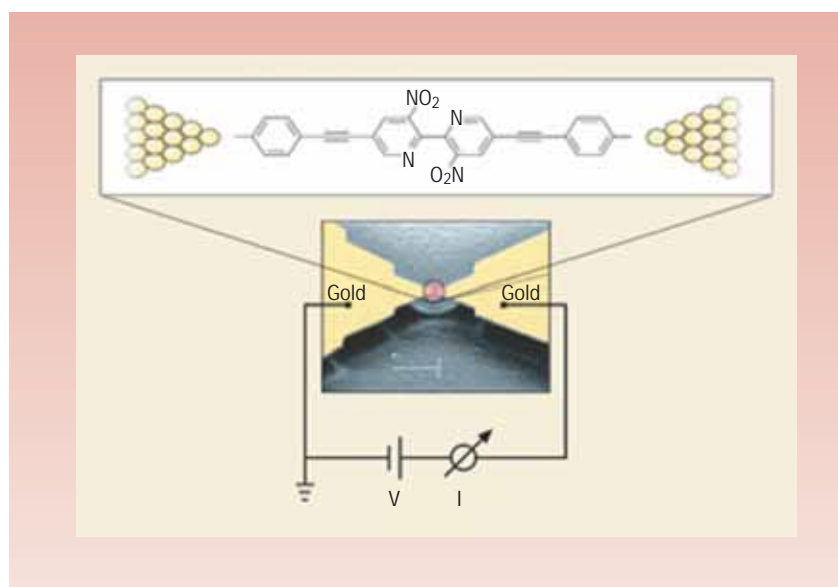
represents the speed with which the new technique could write and read a bit of data—would depend upon the exact mechanism used, Riel said. She noted that the switch could take about 640 microseconds, which would be fast enough for many storage purposes.

Future research will focus on the switching mechanism and the way the design affects storage capabilities, Riel said.

According to Tour, a key issue is that wires and other elements used in conventional computing electronics are too big to use with molecular technology. Researchers will thus have to focus on nanoscale engineering, he added.

Because the research is in such an early stage, the IBM scientists have not yet fully explored how the new technology might work in applications such as memory, noted Riel.

According to Tour, the technique will probably be used in niche applications rather than as a replacement for CMOS technology. ■



IBM has developed a storage device consisting of a single molecule. Researchers placed the bipyridyl dinitro-dithiol molecule between two gold electrodes and applied a current. This caused the voltage flow within the molecule to change, in essence causing the molecule to switch states. This creates the ones and zeros of stored binary data.