

IBM Adds “Nothing” to Chips, Improves Performance

IBM researchers have developed a technique that creates vacuum spaces, called *airgaps*, between the wires in processors using self-assembling technology. These airgaps create a form of insulation that increases the chips’ performance up to 35 percent or reduces their power consumption up to 15 percent.

This is the “first demonstration of a viable airgap technology on a real chip,” said project manager and IBM Fellow Daniel C. Edelstein.

Also, he said, this is the first time self-assembly has been used in a microprocessor-manufacturing environment. This will help chip makers continue making processors smaller, more powerful, and more energy-efficient, as it is becoming increasingly difficult to achieve such gains

via traditional methods such as shrinking transistors or using new lithography approaches.

For years, manufacturers have been shrinking chips’ transistors and wires so that they can pack more of them on processors, making them faster. However, these smaller elements leak current or introduce current to other circuits, which hurts performance, uses additional power, and generates heat. Insulation has thus become an increasingly important issue. IBM’s new approach improves processor insulation.

The airgap technique lowers the chip insulator’s dielectric constant, which describes a material’s ability to transmit charge when a voltage is applied. Because the insulator would transmit less charge, the current

introduced to other circuits would drop. This, explained Edelstein, increases chip performance and reduces energy usage.

The industry has been using glass as an insulator for 40 years. Chip makers have added dopants, including fluorine and carbon, to lower the glass’s dielectric constant—relative to that of a vacuum’s 1.0—to as low as 3.0 generally and to 2.4 in a few cases.

Vacuums are very good insulators because they don’t transmit charge well. Using airgaps between wires can lower a chip insulator’s relative dielectric level to a bit below 2.0, according to Edelstein.

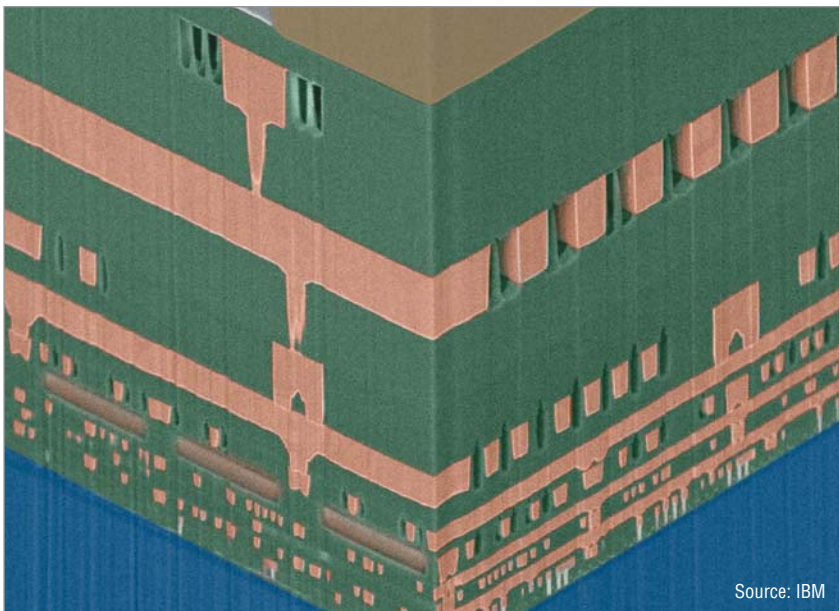
Current lithographic chip-making techniques cannot readily create tiny airgaps for use in processors. Instead of lithography, IBM’s technique uses diblock copolymers, which consist of two polymer strands that arrange themselves in a regular pattern. As the copolymers arrange themselves, they leave an array of tiny airgaps, Edelstein said. This creates a nanometer-scale mesh that Edelstein describes as “a beehive of tiny holes.”

The airgap approach is ideal for the chip-making industry, which is currently emphasizing low-dielectric material for insulation, said Peter Singer, *Semiconductor International* magazine’s editor-in-chief.

However, he said, the idea, at least a decade old, faces manufacturing challenges such as complexity and the possibility that the airgaps could create hot spots or cause potential structural weaknesses. “Also,” he added, “IBM has not said this will be cost-effective. It’s a proof of concept only.”

IBM has built test microprocessors using the new technique, which will be introduced in chips with 32-nanometer feature sizes—initially for use in high-end servers—expected to hit the market in 2009.

IBM’s Research Alliance partners—including Advanced Micro Devices, Sony, and Toshiba—have full access to the technology. And, said Edelstein, “IBM may choose to license to other selected parties.” ■



IBM has developed a technique that creates vacuum spaces, called airgaps, between the wires in processors. This improves the insulation within chips, which raises performance and lowers energy consumption.

Google Surveys Web for Malware

Google has surveyed billions of Web pages in an effort to determine the extent and nature of the online malware problem, which could affect the Internet-based company's many users.

As part of its ongoing study, Google identified in 4.5 million of the surveyed pages factors that indicated they could upload malicious code to a visitor's computer. The company analyzed the pages' HTML source code and also tested them to see how they affected computers.

"We confirmed infections on 450,000 pages," said Google senior staff engineer Niels Provos. "By malware infection, we mean that a user on a vulnerable system could get malware on their computer without their consent just by visiting a Web page."

"This software is often capable of recording the keystrokes that users make and then [capturing] sensitive information such as credit card numbers or bank accounts," he noted.

Google found other malware that could hijack computers and turn them into zombies that a hacker could use remotely to attack other machines. Some of the more harmless infections alter user bookmarks, install toolbars, or change browser start pages.

Ed Skoudis, founder of Intelguardians, an information-security research and consulting company, said that Google found a higher percentage of pages with malware than most expected but that its findings appear to be correct.

New Eye-Tracking Technology Could Make Billboards More Effective

A new portable eye-tracking unit enables outdoor advertisers to more affordably track the effectiveness of a given marketing campaign by accurately measuring the number of people who look at their billboards and video screens.

Xuuk Inc.'s eyebox2, now in commercial release, is an eye-tracking device that monitors the eye movements

of people in motion in real time from up to 10 meters away from an advertisement. Typical eye-tracking machines have not been effective beyond 60 centimeters and have worked best with stationary viewers, making them impractical for outdoor advertisements.

The eyebox2 can also track a series of viewers without requiring recalibration for each new subject, which makes it easy to use.

Moreover, the new technology costs only \$1,000 per system, compared to \$25,000 for typical eye-tracking systems, according to Xuuk (pronounced "zook") CEO Roel Vertegaal, who is also director of the Human Media Laboratory at Canada's Queen's University.

The eyebox2 uses a camera—which connects to a standard PC via a USB port and communicates with the computer via Telnet—mounted atop a display. The use of commodity equipment reduces the system's cost.

The system works over long distances by emitting infrared light and tracking reflections from viewers' eyes, Vertegaal explained. It also works with active-vision technology, which uses sensors and high-speed visual computations to "understand" an environment.

The technology could be used for other advertising- and marketing-related eye-tracking tasks, such as identifying the supermarket-shelf locations that best capture shoppers' attention.

In addition, Vertegaal noted, eyebox2 could be used outside of advertising. For example, if a viewer stops looking at a television screen, the device could pause the program or turn off the TV. ■



The eyebox2 is a portable, long-distance eye-tracking device that can be used for purposes such as determining the number of people who look at billboards. This could help identify the billboards' effectiveness. The eyebox2 emits infrared light and tracks reflections from viewers' eyes.

“Google has a more comprehensive view of the Internet than just about anyone,” he explained. “Also, their [survey] methods look quite solid. Its findings are excellent.”

In addition, to the 450,000 infected pages, Google found another 700,000 that could be considered to contain malware but weren’t identified as such because, for example, they tried but couldn’t successfully download malicious code to a visitor’s computer or performed malicious tasks other than download software.

The research, conducted by Google’s Anti-Malware Team,

proves the need for more users to use antivirus software and automatic security updates, securely configure computers, disable unnecessary features, and take other safety measures that experts have recommended for years, according to Provos.

“Online malware is a problem, so Google’s findings that 10 percent of Web pages it analyzed are infected are not surprising,” said Will Dormann, vulnerability analyst for the CERT Coordination Center at Carnegie Mellon University’s Software Engineering Institute. However, he explained, the findings don’t mean that

10 percent of all Web pages have malware because the company focused on suspicious sites.

“A user who sticks to popular, trusted sites will be at less risk of being the victim of a drive-by download,” he added.

In the majority of cases, Dormann said, malware was placed onto pages after a hacker compromised Web server security.

Also, Provos said, hackers were able to compromise Web servers because of unpatched vulnerabilities or by stealing server-management passwords. ■

Intel Adds Distance to Wi-Fi

Intel Research has developed an approach for producing low-cost systems that extend Wi-Fi wireless technology’s range between antennas from the 100 meters typical in a hot spot to 100 kilometers and, in one test, to 280 km, without losing bandwidth.

The company hopes to use the approach to provide Internet connections, networking services, and other computing technologies to remote parts of the developing world, where building wired infrastructures can be prohibitively difficult and expensive.

There are also applications for the technology in the developed world, noted Eric Brewer, director of Intel Research’s Berkeley Lab. For example, it could be useful in lightly populated rural areas without enough potential customers for providers to want to build costly wired or wireless infrastructures.

“In the developing world and in industrial applications in which cabling is not prevalent or practical,” said analyst Chris Silva with Forrester Research, a market-analysis firm, “the ability to wirelessly connect fixed and mobile network assets is greatly increased by such technologies.”

Wi-Fi systems, implemented via a chip or mini-PCI board, include a

radio, transceiver, antenna, analog-to-digital converter, signal processor, and software.

A standard Wi-Fi antenna is omnidirectional. Because the power is spread in all directions, the range is limited. In Intel’s version, the antennas broadcast all signals directly to another antenna, thereby increasing the range.

In addition, Intel changed Wi-Fi’s signal-transmission technology to time-division multiple access, which lets many users share a single radio channel by assigning each person a unique time slot. Wi-Fi typically uses carrier-sense multiple access, a protocol that enables multiple nodes to transmit on a single channel by letting nodes verify the absence of other traffic before transmitting on the channel. Intel’s use of multiple time slots, as well as packet pipelining, extends Wi-Fi’s range and bandwidth.

The extended Wi-Fi can use a series of point-to-point links between antennas to cover long transmission distances. The system could use these links to connect to other users or an Internet access point.

Intel’s technology works with the IEEE 802.11 a, b, and g flavors of Wi-Fi. It would also work with non-

Intel Wi-Fi systems, as long as they add Intel software.

WiMax is another long-distance, wireless technology that uses multiple antennas. However, the antennas are more expensive. In addition, Wi-Fi might be easier to implement, particularly at a grass-roots level, because governments generally don’t regulate its 2.4 GHz transmission frequency, unlike WiMax’s typical 3.5 GHz frequency. Wi-Fi could even be used to extend WiMax systems affordably, according to Brewer.

Intel’s Wi-Fi technology is being used in Guinea-Bissau, India, the Philippines, and Venezuela. A trial program is under way in Uganda, and a prototype backbone system is under development in Ghana. ■

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