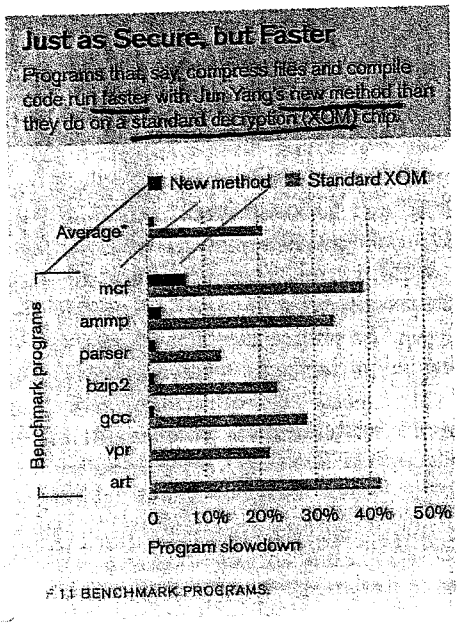
fetched from memory, then decoded, then executed. Jun Yang, an assistant professor of computer science at the University of California, Riverside, and colleagues at Riverside and the University of Texas at Dallas use a security scheme called a one-time pad that can start decryption without the data. The new procedure fetches



data and starts the decryption in parallel, so that the processor can act on instructions almost as they arrive. In a simulation, the extra time needed for decryption dropped from 20.8 percent of the computation time in current XOM processors to a mere 1.3 percent.

WHY IT MATTERS: Until now, the XOM fix caused a performance slowdown of as much as 42 percent. For some applications, like ATMs and other financial systems, it's worth the cost. But for interactive applications like video games, sluggish response times—reminiscent of surfing the Internet in the early days—simply are not acceptable. Yang and colleagues' technique faces sizable hurdles to adoption: devices will need updated software and new processors with extra on-chip memory. Nevertheless, the researchers' method for improving the performance of encrypted software might be the breakthrough required to produce systems that are both secure and fast.

Source: Yang, J., et al. 2005. Improving memory encryption performance in secure processors. *IEEE Transactions on Computers* 54:630–640.

Timing Text

Mobile messaging on cue

CONTEXT: Some text messages, like birthday wishes or driving directions, make sense only in particular contexts. But cell phones send messages immediately, not when they are most timely. Younghee Jung, Per Persson, and Jan Blom of Nokia have now designed cell-phone software that lets senders dictate when and where their text messages should be delivered.

METHODS AND RESULTS: Cell phones already track what time it is, where they are, and who has called recently. Jung and colleagues wrote software that monitors this information and withholds messages until certain delivery conditions are met. They designed a user interface that lets senders choose conditions such as time of day or a recipient's location. Finally, they loaded the software onto phones, gave them to seven Finnish teens, and monitored their use over several weeks.

More than 10 percent of all sent messages used this "context-enhanced" delivery. Just over half of these were triggered by the recipient's location—in, say, the vicinity of a common rendezvous point. Most of the rest specified when a message should be delivered, and many were timed to reach friends when they were in between known engagements.

WHY IT MATTERS: Context-specific delivery could change the way people use cell phones. However, the change could be as much a curse as a benefit. Although the teens' biggest complaint was that they couldn't be sure friends received their messages, the researchers haven't yet identified a way to verify delivery that protects the recipient's privacy. If a phone sends a confirmation when a message is read, it will also reveal where the recipient is. Vendors might also be tempted to send messages that would be delivered as users neared their shops' locations, creating a boom in text-message spam.

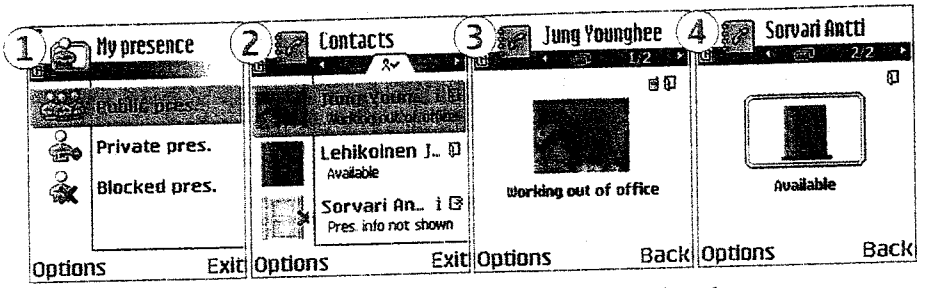
Source: Jung, Y., et al. 2005. DeDe: design and evaluation of a context-enhanced mobile messaging system. Paper presented at Conference on Human Factors in Computing Systems. April 2–7. Portland, OR.

Smoothing Out Speech

Internet phones get clearer

CONTEXT: People trying to converse over wireless local-area networks (WLANs)—using them to connect to voice-over-Internet-protocol, or VoIP, systems—are often confounded by the poor quality of the transmission. Those frustrations may soon clear up, thanks to researchers at the University of California, Santa Barbara, who report a method to improve the clarity of VoIP conversations.

METHODS AND RESULTS: Information is sent over a WLAN network in units called packets. But wireless signals can deteriorate over distance, interfere with each other, or otherwise introduce errors into the packets. If that happens, the transmission standard IEEE 802.11 requires that the packets be re-sent. The subsequent delay garbles real-time communication. While zero error tolerance makes sense for e-mail, it might be too strict a standard for voice: Ian Chakeres and colleagues have shown that digitized voice data can



Nokia's cell-phone interface (1) lets users specify times and locations for delivering text messages. A scroll-down menu (2) displays the status of the user's contacts (3, 4).

COURTESY OF NOKIA

COURTESY OF *NATURE NEUROSCIENCE*