24.94x12.06	54	עמוד 6	THE JERUSALEM POST - FRONT	01/01/2012	30223343-0
מכון ויצמן למדע - 12033					

Up in a cloud for processing computer data

A declining amount of computing is conducted today on desktop computers; instead, cloud computing – in which operations are carried out on a network of shared, remote servers – is expected to rise as the demand for computing power increases. This raises some crucial questions about security: For instance, can we perform computations on data stored in the "cloud" without letting anyone else see our information?

Research carried out at the Weizmann Institute of Science in Rehovot and the Massachusetts Institute of Technology is moving us closer to the ability to work on data while it is still encrypted, giving an encrypted result that can later be securely deciphered.

Attempting computation on sensitive data stored on shared servers leaves that data exposed in ways that traditional encryption techniques can't prevent. The main problem is that to manipulate the data, it has to be first decoded. "Until a few years ago, no one knew if the encryption needed for this sort of online security was even possible," says Dr. Zvika Brakerski, who recently completed his Ph.D. under Prof. Shafi Goldwasser of the computer science and applied mathematics department.

In 2009, however, a doctoral student at Stanford University named Craig Gentry provided the first demonstration of so-called fully homomorphic encryption (FHE). His original method was extraordinarily time-consuming and unwieldy, making it highly impractical. Gentry constructed his FHE system by using fairly sophisticated math, based on so-called "ideal lattices," and this required him to make new and unfamiliar complexity assumptions to prove security. Gentry's use of ideal lattices seemed inherent to FHE; researchers assumed that they were necessary for the server to perform such basic operations as addition and multiplication on encrypted data.

NEW WORLDS

• By JUDY SIEGEL-ITZKOVICH

Brakerski, together with Dr. Vinod Vaikuntanathan (who was Goldwasser's student at MIT), surprised the computer security world earlier this year with two scientific papers in which they described several new ways of making fully homomorphic encryption more efficient. For one thing, they managed to make FHE work with much simpler arithmetic, which speeds up processing time. And a surprise discovery showed that a mathematical construct used to generate the encryption keys could be simplified without compromising security. Gentry's original ideal lattices are theoretical collections of points that can be added together – as in an ordinary lattice structure – and also multiplied. But the new research shows that the lattice does not have to be ideal, which simplifies the construction immensely. "The fact that it worked was something like magic, and it has challenged our assumptions about the function of the ideal lattices in homomorphic encryption," says Brakerski.

Their result promises to pave a path to applying FHE in practice. Optimized versions of the new system could be hundreds – or even thousands – of times faster than Gentry's original construction. Indeed, Brakerski and Vaikuntanathan have managed to advance the theory behind fully homomorphic encryption to the point that computer engineers can begin to work on applications. These might include, for instance, securing medical information for research: A third party could perform large medical studies on encrypted medical records without having access to the individuals' information.