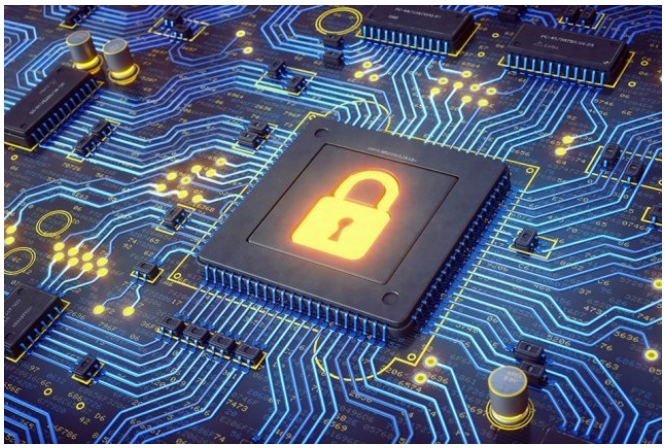
Energy-efficient encryption for the internet of things

13 February 2018, by Larry Hardesty



MIT researchers have built a new chip, hardwired to perform public-key encryption, that consumes only 1/400 as much power as software execution of the same protocols would. It also uses about 1/10 as much memory and executes 500 times faster. Credit: Massachusetts Institute of Technology

Most sensitive web transactions are protected by public-key cryptography, a type of encryption that lets computers share information securely without first agreeing on a secret encryption key.

Public-key encryption protocols are complicated, and in computer networks, they're executed by software. But that won't work in the internet of things, an envisioned network that would connect many different sensors—embedded in vehicles, appliances, civil structures, manufacturing equipment, and even livestock tags—to online servers. Embedded sensors that need to maximize battery life can't afford the energy and memory space that software execution of encryption protocols would require.

MIT researchers have built a new chip, hardwired to perform public-key encryption, that consumes only 1/400 as much power as software execution of the same protocols would. It also uses about 1/10 as much memory and executes 500 times faster. The researchers describe the chip in a paper they're presenting this week at the International Solid-State Circuits Conference.

Like most modern public-key encryption systems, the researchers' chip uses a technique called elliptic-curve encryption. As its name suggests, elliptic-curve encryption relies on a type of mathematical function called an elliptic curve. In the past, researchers—including the same MIT group that developed the new chip—have built chips hardwired to handle specific elliptic curves or families of curves. What sets the new chip apart is that it is designed to handle any elliptic curve.

"Cryptographers are coming up with curves with different properties, and they use different primes," says Utsav Banerjee, an MIT graduate student in electrical engineering and computer science and first author on the paper. "There is a lot of debate regarding which curve is secure and which curve to use, and there are multiple governments with different standards coming up that talk about different curves. With this chip, we can support all of them, and hopefully, when new curves come along in the future, we can support them as well."

Joining Banerjee on the paper are his thesis advisor, Anantha Chandrakasan, dean of MIT's School of Engineering and the Vannevar Bush Professor of Electrical Engineering and Computer Science; Arvind, the Johnson Professor in Computer Science Engineering; and Andrew Wright and Chiraag Juvekar, both graduate students in electrical engineering and computer science.

Modular reasoning

To create their general-purpose elliptic-curve chip, the researchers decomposed the cryptographic computation into its constituent parts. Elliptic-curve cryptography relies on modular arithmetic, meaning

that the values of the numbers that figure into the computation are assigned a limit. If the result of some calculation exceeds that limit, it's divided by the limit, and only the remainder is preserved. The secrecy of the limit helps ensure cryptographic security.

One of the computations to which the MIT chip devotes a special-purpose circuit is thus modular multiplication. But because elliptic-curve cryptography deals with large numbers, the chip's modular multiplier is massive. Typically, a modular multiplier might be able to handle numbers with 16 or maybe 32 binary digits, or bits. For larger computations, the results of discrete 16- or 32-bit multiplications would be integrated by additional logic circuits.

The MIT chip's modular multiplier can handle 256-bit numbers, however. Eliminating the extra circuitry for integrating smaller computations both reduces the chip's energy consumption and increases its speed.

Another key operation in elliptic-curve cryptography is called inversion. Inversion is the calculation of a number that, when multiplied by a given number, will yield a modular product of 1. In previous chips dedicated to elliptic-curve cryptography, inversions were performed by the same circuits that did the modular multiplications, saving chip space. But the MIT researchers instead equipped their chip with a special-purpose inverter circuit. This increases the chip's surface area by 10 percent, but it cuts the power consumption in half.

The most common encryption protocol to use elliptic-curve cryptography is called the datagram transport layer security protocol, which governs not only the elliptic-curve computations themselves but also the formatting, transmission, and handling of the encrypted data. In fact, the entire protocol is hardwired into the MIT researchers' chip, which dramatically reduces the amount of memory required for its execution.

The chip also features a general-purpose processor that can be used in conjunction with the dedicated circuitry to execute other elliptic-curve-based security protocols. But it can be powered down when not in use, so it doesn't compromise the chip's energy efficiency.

"They move a certain amount of functionality that used to be in software into hardware," says Xiaolin Lu, director of the internet of things (IOT) lab at Texas Instruments. "That has advantages that include power and cost. But from an industrial IOT perspective, it's also a more user-friendly implementation. For whoever writes the software, it's much simpler."

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology