10

To make solid-state batteries that are practical and inexpensive to produce, Sastry has written simulation software to identify combinations of materials and structures that will yield compact, reliable high-energy devices. She can simulate these materials and components precisely enough to accurately predict how they will behave when assembled together in a battery cell. She is also developing manufacturing techniques that lend themselves to mass production. "If your overall objective is to change the way people drive, your criteria can no longer only be the best energy density ever achieved or the greatest number of cycles," she says. "The ultimate criterion is affordability, in a product that has the necessary performance."

Although it may be several years before the batteries come to market, GM and other major automakers, such as Toyota, have already identified solid-state batteries as a potentially key component of future electric vehicles. There's a limit to how much better conventional batteries can get, says Jon Lauckner, president of GM Ventures, which pumped over $3 million into Sakti3 last year. If electric vehicles are ever to make up more than a small fraction of cars on the road, "something fundamental has to change," he says. He believes that Sakti3 is "working well beyond the limits of conventional electrochemical cells."

Sastry is aware that success isn't guaranteed. Her field is something of a technological battleground, with many different approaches competing to power a new generation of cars. "None of this is obvious," she says. *—Kevin Bullis*

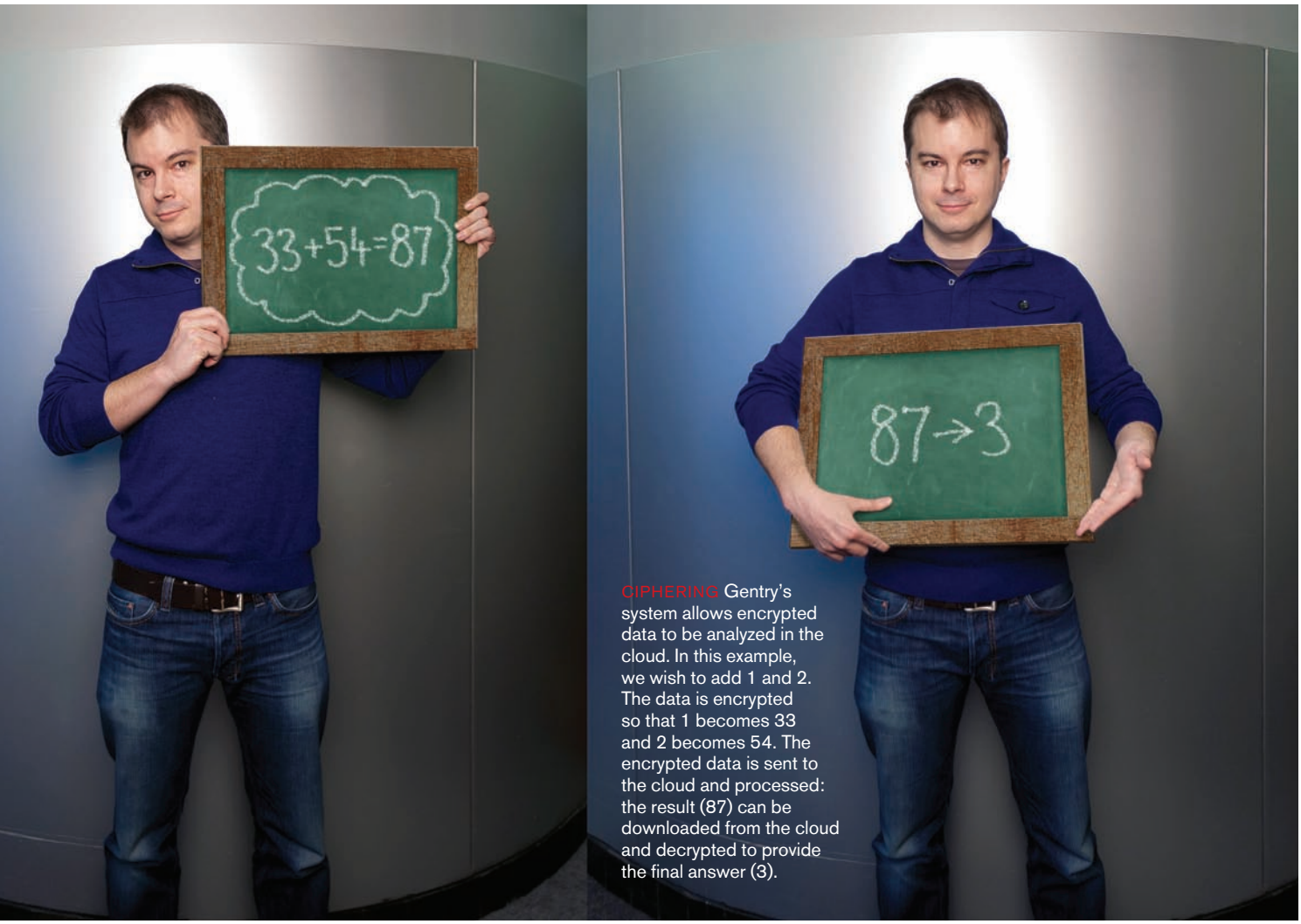
ANN MARIE SASTRY
(Sakti3) Smaller and lighter lithium batteries will make electric vehicles more competitive.

OTHERS WORKING ON SOLID-STATE BATTERIES
Planar Energy, Orlando, Florida
Seeo, Berkeley, California
Toyota, Toyota City, Japan

Making cloud computing more secure
Homomorphic Encryption

Craig Gentry is creating an encryption system that could solve the problem keeping many organizations from using cloud computing to analyze and mine data: it's too much of a security risk to give a public cloud provider such as Amazon or Google access to unencrypted data.

The problem is that while data can be sent to and from a cloud provider's data center in encrypted form, the servers that power a cloud can't do any work on it that way. Now Gentry, an IBM researcher, has shown that it *is* possible to analyze data without decrypting it. The key is to encrypt the data in such a way that performing a mathematical operation on the encrypted information and then decrypting the result produces the same answer as performing an analogous operation on the unencrypted data. The correspondence between the oper-



CIPHERING Gentry's system allows encrypted data to be analyzed in the cloud. In this example, we wish to add 1 and 2. The data is encrypted so that 1 becomes 33 and 2 becomes 54. The encrypted data is sent to the cloud and processed: the result (87) can be downloaded from the cloud and decrypted to provide the final answer (3).

STEVE MOORS

ations on unencrypted data and the operations to be performed on encrypted data is known as a homomorphism. "In principle," says Gentry, "something like this could be used to secure operations over the Internet."

With homomorphic encryption, a company could encrypt its entire database of e-mails and upload it to a cloud. Then it could use the cloud-stored data as desired—for example, to search the database to understand how its workers collaborate. The results would be downloaded and decrypted without ever exposing the details of a single e-mail.

Gentry began tackling homomorphic encryption in 2008. At first he was able to perform only a few basic operations on encrypted data before his system started producing garbage. Unfortunately, a task like finding a piece of text in an e-mail requires chaining together thousands of basic operations. His solution was to use a second layer of encryption, essentially to protect intermediate results when the system broke down and needed to be reset.

"The problem of how to create true homomorphic encryption has been debated for more than 30 years, and Craig was the first person who got it right and figured out how to make the math work," says Paul Kocher, the president of the security firm Cryptography Research. However, Kocher warns, because Gentry's scheme currently requires a huge amount of computation, there's a long way to go before it will be widely usable.

Gentry acknowledges that the way he applied the double layer of encryption was "a bit of a hack" and that the system runs too slowly for practical use, but he is working on optimizing it for specific applications such as searching databases for records. He estimates that these applications could be ready for the market in five to 10 years. *—Erica Naone*

CRAIG GENTRY
(IBM) A secure way to process data could encourage more enterprises to use cloud computing.

OTHERS WORKING ON HOMOMORPHIC ENCRYPTION
Marten van Dijk, MIT, Cambridge, Massachusetts
Eleanor Reiffel, Fuji Xerox Palo Alto Research Laboratory, California
Nigel Smart, Bristol University, U.K.