Forbes.com

Breakthroughs

IBM's Blindfolded Calculator

Andy Greenberg, 07.13.09, 12:00 AM ET

---© Evan Kafka

The computer science problems that earned Craig Gentry his job at **IBM** sound a bit like Zen koans. Could **Google** search the Web without knowing what it was looking for? Can an e-mail filter identify spam without reading it? Could an official count votes in an election without opening a ballot?

Those privacy puzzles, as Gentry has shown in an unpublished Ph.D. dissertation, aren't as paradoxical as they seem. In a cryptographic epiphany last summer, the 35-year-old IBM researcher cracked a problem that had remained unanswered despite 30 years of cryptographers' attention. His algorithm promises to unlock fertile new tangents in computer science and may eventually put IBM's stamp on a new blend of computation and privacy.

The premise of what computer scientists call "fully homomorphic encryption," like many long-unsolved mathematical puzzles, sounds both simple and impossible: Can data be encrypted in a way that allows any calculation to be performed on the scrambled information without unscrambling it?

Imagine online accounting software that takes in encrypted data about your salary and expenditures, crunches the numbers and spits out an encrypted tax filing ready to be decrypted and sent to the IRS. The accounting software would never know the contents of what it had

analyzed, and you might be less fretful about sending sensitive financial data to that online tax service.

"It's like one of those boxes with the gloves that are used to handle toxic chemicals," says Gentry. "All the manipulation happens inside the box, and the chemicals are never exposed to the outside world."

You can, of course, keep your tax return secret from your accountant by running the tax software on your own computer. An e-mail filter that directs all messages about a confidential merger plan to a particular folder could run locally, too. But the trend in computing today is moving data and applications like tax accounting and e-mail filtering off the desktop to independently owned data centers--the so-called "cloud." That shift makes better use of scarce resources and also means that your files are always at your fingertips, no matter where you are or what device you're using. For cloud computing to fulfill its promises, users need more confidence that their secrets will stay secret. That's where Gentry's discovery fits in, though it could take another decade to put his theory into practice.

Homomorphic encryption, like any encryption, mathematically scrambles data so thoroughly that the unscrambling can be done only by someone possessing a secret key. But even though the encryption seems to produce chaos, it might preserve certain mathematical relationships among the possible inputs. If the encrypted version of input x, multiplied by the encrypted version of input y, equals the encrypted version of x times y, then the process is said to be homomorphic with respect to multiplication.

Fully homomorphic encryption would preserve not just multiplication but also addition. What's the point of that tweak? Any computer algorithm--whether it sorts your mail or figures out whether you qualify for a tax deduction--boils down to a series of arithmetic steps. If an encryption scheme allowed any number of additions or multiplications, any computing application would be possible without decrypting data.

The idea of fully homomorphic encryption was first posited in a paper three decades ago by Ronald Rivest, an MIT professor and the coinventor of the famous RSA encryption scheme now ubiquitous in business transactions. Rivest and his two coauthors also suggested it was probably impossible.

Gentry approached the mathematical riddle from an unusual path. A graduate of Harvard Law School with a bachelor's degree in math, he'd been bored with practicing intellectual-property law. In 2005 Gentry enrolled in Stanford's Ph.D. program, and in June of 2008 took a three-month internship with IBM.

Gentry's fully homomorphic revelation came to him as he sat in a New York City cafe that summer. The encryption method that intrigued him allows a few multiplications or additions of encrypted data. But it suffers from an interesting handicap. Every arithmetic step unavoidably introduces small amounts of error into the encrypted data. Performing just a dozen or so computations corrupts the data to the degree that it can no longer be accurately decrypted.

Gentry's insight was to double-encrypt the data in such a way that the errors could be removed, so to speak, in the dark. By periodically unlocking the inner layer of encryption underneath an outer layer of scrambling, the cloud computer would clean up its messes as it went along, without ever seeing the secret data. It took Gentry another 15 minutes to realize that he'd just solved an epic cryptographic problem.

Gentry's elegant solution has a catch: It requires immense computational effort. In the case of a Google search, for instance, performing the process with encrypted keywords would multiply the necessary computing time by around 1 trillion, Gentry estimates. But now that Gentry has broken the theoretical barrier to fully homomorphic encryption, the steps to make it practical won't be far behind, predicts professor Rivest. "There's a lot of engineering work to be done," he says. "But until now we've thought this might not be possible. Now we know it is."

Today the barrier to business adoption of encryption isn't that the techniques need to be stronger. By all known methods, a million pcs would take more than a hundred years to decode a single number scrambled with an RSA encryption using a 4,096-bit key. Instead, Gentry and others argue that encryption needs to be more adaptable. "If you have to decrypt your data to actually use it, no one's going to encrypt in the first place," he says. "Inflexible encryption is basically just an obstacle."

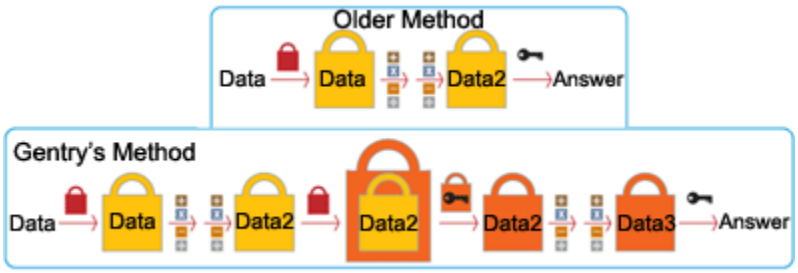
A 2008 study by the privacy-focused Ponemon Institute found that only 21% of U.S. businesses and government agencies had a consistent encryption policy across all parts of their organizations. Meanwhile, over the last six months U.S. government and private-sector entities lost more than 12 million files containing sensitive personal data to hackers, thieves and careless employees, according to the Identity Theft Resource Center.

Ending that data hemorrhaging--and delivering on the promise of cloud computing--will require not only stronger encryption but also smarter encryption. Developing those adaptable cryptography methods isn't a matter of putting more thought into cryptography as much as it is approaching old problems differently--so says Daniel Boneh, the Stanford professor who got Gentry thinking about homomorphisms.

"The community is going one way, and then one smart guy like Craig looks in a different direction. That's how breakthroughs happen," Boneh says. "You look down some other path, and suddenly everything that had seemed impossible becomes possible."

Crypto Trickery

Older encryption schemes can do only a few calculations before corrupting data to the degree that it can't be decrypted. Gentry's method adds another layer of encryption every few steps and uses an encrypted key to unlock the inner layer of scrambling. That decryption "refreshes" the data without exposing it, allowing an infinite number of computations.



Read William Baldwin's Sidelines On This Story

Side Lines
Encrypt Your Phone Calls
William Baldwin, 07.13.09

The century-old arms race between law enforcement and privacy is heating up. Who wins? Who should win?

Your answer to the second question depends on who's trying to keep his communications private. In the 2006 movie *Das Leben der Anderen*, the bad guys are the secret police, snooping on dissidents. In the digital battlegrounds of Tehran and Tiananmen, you root for the privacy seekers.

But what if the subject of the bugging is a gang of terrorists planning to blow up a synagogue? Or a crooked governor selling a Senate seat? Then you realize that a victory for privacy would not be an unmixed blessing.

Like it or not, privacy is going to win this battle. One reason is that mathematics favors the cipher. Add a few arithmetic steps to your encrypting program and you slow down your computer by a few seconds but delay the code crackers by a few thousand years. In his column Lee Gomes looks at encryption from the everyday perspective of a Microsoft Office user. For people who take the trouble to use long passwords, security has gotten very, very good. In "Super Secret Encryption" Andy Greenberg explores a breakthrough in coding that, while purely theoretical today, could someday lead to better privacy in a world where most of your personal computation takes place at a far remove from your desktop.

The other factor is the likely drift of the telephone network to the Internet Protocol, the format used by Skype. Voice over IP converts conversations to packets of bits that can be easily encrypted with secret keys invented on the fly. Code your phone calls and all the wiretap warrants in the world won't allow the FBI to listen in.

Chief proponent of encrypting phone calls is Philip Zimmermann, whose Zfone software handles all the details. Mainstream phone companies are for now just sniffing at the idea, but it's quite possible that, in a world of IP telephony a decade hence, encryption will become the default option.

Zimmermann is a hero to privacy fans for winning a battle with the government in the 1990s over his Pretty Good Privacy encryption program. The feds thought PGP was so powerful that it should be regulated as a munitions export. They eventually backed down. They had to. Encryption these days boils down to some well-known computational tricks. It's one thing to stop a missile launcher at the border, quite another to interdict an equation.

Outlaw encryption? That would be not only impossible but a big mistake. So much business these days hangs on secure transmission--your Amazon order, bank wire transfers, government purchasing. Yes, al Qaeda uses encryption. Bank robbers use getaway cars, but that doesn't mean we should outlaw the automobile. In the next century the law enforcers are simply going to have to live without wiretaps.