A basis for all cryptography

October 28 2015, by Larry Hardesty

"Indistinguishability obfuscation" is a powerful concept that would yield provably secure versions of every cryptographic system we've ever developed and all those we've been unable to develop. But nobody knows how to put it into practice.

Last week, at the IEEE Symposium on Foundations of Computer Science, MIT researchers showed that the problem of indistinguishability obfuscation is, in fact, a variation on a different cryptographic problem, called efficient functional encryption. And while computer scientists don't know how to do efficient functional encryption, either, they believe that they're close—much closer than they thought they were to indistinguishability obfuscation.

"This thing has really been studied for a longer time than obfuscation, and we've had a very nice progression of results achieving better and better functional-encryption schemes," says Nir Bitansky, a postdoc in MIT's Computer Science and Artificial Intelligence Laboratory who wrote the conference paper together with Vinod Vaikuntanathan, an associate professor of electrical engineering and computer science. "People thought this is a small gap. Obfuscation—that's another dimension. It's much more powerful. There's a huge gap there. What we did was really narrow this gap. Now if you want to do obfuscation and get all of crypto, everything that you can imagine, from standard assumptions, all that you have to do is solve this very specific problem, making functional encryption just a little bit more efficient."

In computer science, "obfuscation" means disguising the operational details of a computer program so that it can't be reverse-engineered. Many obfuscation techniques have been proposed, and many have been broken.

So computer scientists began investigating the idea theoretically. The ideal obfuscation scheme would take the source code for a program and rewrite it so that it still yields a working program, but it is impossible to determine what operations it was executing.

Theorists quickly proved that ideal obfuscation would enable almost any cryptographic scheme that they could dream up. But almost as quickly, they proved that it was impossible: There's always a way to construct a program that can't be perfectly obfuscated.

Fuzzy details

So they began investigating less-stringent theoretical principles, one of which was indistinguishability obfuscation. Rather than requiring that an adversary have no idea what operations the program is executing, indistinguishability obfuscation requires only that the adversary be unable to determine which of two versions of an operation it's executing.

Most people recall from algebra, for instance, that a x (b + c) is the same thing as (a x b) + (a x c). For any given values, both expressions yield the same result, but they'd be executed differently on a computer. Indistinguishability obfuscation permits the adversary to determine that the program is performing one of those computations, but not which.

For years, the idea of indistinguishability obfuscation lay idle. But in the last few years, computer scientists have shown how to construct indistinguishability-obfuscation schemes from mathematical objects called multilinear maps. Remarkably, they also showed that even the weaker notion of indistinguishability obfuscation could yield all of cryptography.

But multilinear maps are not well understood, and it's not clear that any of the proposed techniques for building them will offer the security guarantees that indistinguishability obfuscation requires.

Tip of the iceberg

Functional encryption, on the other hand, has for decades been a popular research topic in cryptography. It's a method for performing some operation on an encrypted file, with an intelligible result, but without leaking any further information about the file's contents. It could, for instance, allow a server hosting a wealth of encrypted e-mails to decrypt just the senders' names, for search purposes.

With a standard encryption scheme, encryption time is proportional to the length of the file being encrypted. That's what Bitansky and Vaikuntanathan mean by "efficient." But the best functional-encryption schemes aren't quite that good: Their encryption efficiencies also include a factor proportional to the size of the result of the operation. If the operation were the decryption of the sender's name, that factor would be pretty small. But in principle, it could be much larger.

Bitansky acknowledges that researchers may have underestimated the difficulty of eliminating that extra factor. "It could be that our initial view of the world was false," he says. "Maybe this is not such an easy problem. Maybe this is the real gap, and it could take a very long time to solve. But I'm an optimist."

"Our current candidate constructions for IO [indistinguishability obfuscation] are all based on very new and not-well-understood assumptions that may very well be broken in the near future—and indeed, many of them have been broken," says Rafael Pass, an associate professor of computer science at Cornell University. "Functional encryption is a significantly simpler-looking primitive, so this work opens a new avenue for getting secure constructions of IO."

"The technical approach is simple and beautiful, and I expect it will have lots of other applications," Pass adds.

More information: Indistinguishability Obfuscation from Functional Encryption. eprint.iacr.org/2015/163.pdf

Citation: A basis for all cryptography (2015, October 28) retrieved 16 August 2024 from https://phys.org/news/2015-10-basis-cryptography.html