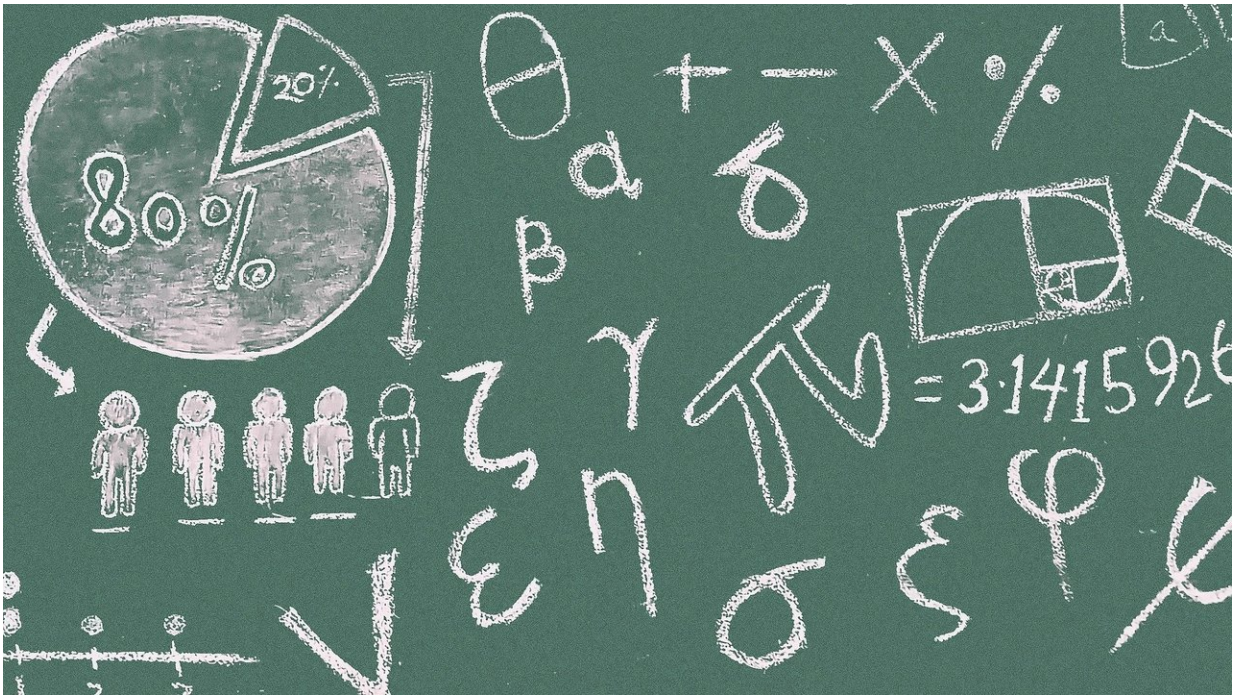
Answer to thorny question could unlock internet security

August 12 2021, by Tom Fleischman



Credit: CC0 Public Domain

Is it easier to check that a solution to a problem is correct than it is to solve the problem?

The question—known as the "NP versus P" problem—is the deepest fundamental problem in computer science and cryptography, lying at the heart of whether any internet data can ever be truly private.

In the unlikely event that P = NP, all encryption schemes and methods of keeping our data on the internet private would be insecure. But even if P is not equal to NP, and even if someone manages to prove this, we still don't know how to get an encryption scheme that is truly secure.

Rafael Pass, professor of computer science at Cornell Tech and at the Cornell Ann S. Bowers College of Computing and Information Science, and co-author Yanyi Liu, a doctoral student in the field of computer science, have offered a solution—sort of.

Their work is detailed in "On the Possibility of Basing Cryptography on EXP ≠ BPP," which won the Best Paper award at CRYPTO '21 and will be presented at the conference Aug. 17.

The question posed in the title of the paper deals with the idea of randomness, a thorny computer science and math question. The EXP versus BPP problem—while not as famous as "NP versus P"– is another longstanding open problem, and cause for even more embarrassment in the field, according to Pass.

"The question essentially is, can randomness exponentially speed up computations?" Pass said. "That's clearly believed to be impossible. We wouldn't think that just tossing some random coins will allow us to speed up our computations exponentially. That would be kind of crazy, but people still have not been able to prove that."

If computations can be exponentially sped up using randomness then all encryption schemes can be broken. The so-called "brute-force" attacks, in which all possible keys are enumerated, could now be efficiently implemented.

Pass and Liu tackle the question of whether simply assuming that EXP is not equal to BPP—that computations cannot be exponentially sped up

using randomness—suffices to get unbreakable encryption schemes. Toward this, Pass and Liu revisit a connection between encryption schemes and time-bounded Kolmogorov Complexity that they established last year.

The time-bounded Kolmogorov Complexity of a string (x) is the length of the shortest program that can output x in a set amount of time. But the new work considers a different notion of Kolmogorov complexity: computing the "Levin-Kolmogorov Complexity" of a string (x). The problem: Given x, find the "most efficient" program that prints x, where "efficiency" is the sum of the length of the program and the logarithm of the running time of the program.

Their paper shows that unbreakable encryptions are possible if and only if there does not exist an efficient algorithm that can compute the Levin-Kolmogorov Complexity for most strings, without making too many mistakes.

"So to get an unbreakable encryption," Pass said, "we just need to show that no efficient algorithm can solve this particular problem."

While they are not able to prove that no such algorithm exists, they show that assuming EXP is not equal to BPP, there does not exist an efficient "errorless" algorithm (an algorithm that either produces the correct answer or says "I don't know") for determining the Levin-Kolmogorov Complexity of a large fraction of random strings.

"It doesn't have to solve it for all the strings—it can give up sometimes," Pass said. "But when it gives an answer, it always needs to be the correct one."

In other words, algorithms that may err do great on tests where you are rewarded based on the number of questions you get right, whereas

errorless algorithms also do well on tests where you are penalized for questions you get wrong.

Their results conclude that the Levin-Kolmogorov Complexity problem is central for understanding both the EXP versus BPP problem, and the problem of whether unbreakable encryption schemes exist.

"This problem holds the key to some of the most important questions in computer science," Pass said. "This specific problem is fundamental and we really need to understand the gap between errorless algorithms and algorithms that may err."

The authors show that if the gap can be closed—a gigantic "if" in computer science—then you have not only proven that unbreakable cryptography exists if EXP does not equal BPP, but in fact you have also proven that NP is not equal to P.

More information: Yanyi Liu and Rafael Pass, On the Possibility of Basing Cryptography on EXP 6 ≠ BPP. eprint.iacr.org/2021/535.pdf

Provided by Cornell University