New method of producing random numbers could improve cybersecurity

May 16 2016

An important application for random numbers is in generating keys for data encryption that are hard for hackers to crack. Credit: James Bowe, via Create Commons Attribution 2.0 Generic license.

With an advance that one cryptography expert called a "masterpiece," University of Texas at Austin computer scientists have developed a new method for producing truly random numbers, a breakthrough that could be used to encrypt data, make electronic voting more secure, conduct statistically significant polls and more accurately simulate complex systems such as Earth's climate.

The new method creates truly random numbers with less computational effort than other methods, which could facilitate significantly higher levels of security for everything from consumer credit card transactions to military communications.

Computer science professor David Zuckerman and graduate student Eshan Chattopadhyay will present research about their method in June at the annual Symposium on Theory of Computing (STOC), the Association for Computing Machinery's premier theoretical computer science conference. An invitation to present at the conference is based on a rigorous peer review process to evaluate the work's correctness and significance. Their paper will be one of three receiving the STOC Best Paper Award.

"This is a problem I've come back to over and over again for more than 20 years," says Zuckerman. "I'm thrilled to have solved it."

Chattopadhyay and Zuckerman publicly released a draft paper describing their method for making random numbers in an online forum last year. In a field more accustomed to small, incremental improvements, the computer science community hailed the method, suggesting that, compared with earlier methods, this one is light years ahead. Oded Goldreich, a professor of computer science at the Weizmann Institute of Science in Israel, commented that even if it had only been a moderate improvement over existing methods, it would have justified a "night-long party."

"When I heard about it, I couldn't sleep," says Yael Kalai, a senior researcher working in cryptography at Microsoft Research New England who has also worked on randomness extraction. "I was so excited. I couldn't believe it. I ran to the (online) archive to look at the paper. It's really a masterpiece."

The new method takes two weakly random sequences of numbers and turns them into one sequence of truly random numbers. Weakly random sequences, such as air temperatures and stock market prices sampled over time, harbor predictable patterns. Truly random sequences have nothing predictable about them, like a coin toss.

The new research seems to defy that old adage in computer programming, "Garbage in, garbage out." In fact, it's the latest, most powerful addition to a class of methods that Zuckerman pioneered in the 1990s called randomness extractors.

Previous versions of randomness extractors were less practical because they either required that one of the two source sequences be truly random (which presents a chicken or the egg problem) or that both source sequences be close to truly random. This new method sidesteps both of those restrictions and allows the use of two sequences that are only weakly random.

An important application for random numbers is in generating keys for data encryption that are hard for hackers to crack. Data encryption is critical for making secure credit card purchases and bank transactions, keeping personal medical data private and shielding military communications from enemies, among many practical applications.

Zuckerman says that although there are already methods for producing high-quality random numbers, they are very computationally demanding. His method produces higher quality randomness with less effort.

"One common way that encryption is misused is by not using high-quality randomness," says Zuckerman. "So in that sense, by making it easier to get high-quality randomness, our methods could improve security."

Their paper shows how to generate only one truly random number—akin to one coin toss—but Zuckerman's former student Xin Li has already demonstrated how to expand it to create sequences of many more random numbers.

The website where Zuckerman and Chattopadhyay posted their draft last summer, called the Electronic Colloquium on Computational Complexity, allows researchers to share their work and receive feedback before publishing final versions in journals or at conferences. Computer scientists and mathematicians have been carefully reviewing the article, providing suggestions and even extending the method to make it more powerful.

Provided by University of Texas at Austin

Citation: New method of producing random numbers could improve cybersecurity (2016, May 16) retrieved 2 May 2024 from https://phys.org/news/2016-05-method-random-cybersecurity.html