Post-quantum cryptography program enters 'selection round'

July 23 2020

A select few algorithms, some of which fall into one of three mathematical "families," are undergoing a final leg of review. Some will form the core of the first post-quantum cryptography standard. Credit: B. Hayes/NIST

The race to protect sensitive electronic information against the threat of quantum computers has entered the home stretch.

After spending more than three years examining new approaches to encryption and data protection that could defeat an assault from a quantum computer, the National Institute of Standards and Technology (NIST) has winnowed the 69 submissions it initially received down to a final group of 15. NIST has now begun the third round of public review. This "selection round" will help the agency decide on the small subset of these algorithms that will form the core of the first post-quantum cryptography standard.

"At the end of this round, we will choose some algorithms and standardize them," said NIST mathematician Dustin Moody. "We intend to give people tools that are capable of protecting sensitive information for the foreseeable future, including after the advent of powerful quantum computers."

The latest details on the project appear in the Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process (NISTIR 8309), which was published today. NIST is asking experts to provide their input on the candidates in the report.

"We request that cryptographic experts everywhere focus their attention on these last algorithms," Moody said. "We want the algorithms we eventually select to be as strong as possible."

Classical computers have many strengths, but they find some problems intractable—such as quickly factoring large numbers. Current cryptographic systems exploit this difficulty to protect the details of online bank transactions and other sensitive information. Quantum computers could solve many of these previously intractable problems easily, and while the technology remains in its infancy, it will be able to defeat many current cryptosystems as it matures.

Because the future capabilities of quantum computers remain an open

question, the NIST team has taken a variety of mathematical approaches to safeguard encryption. The previous round's group of 26 candidate algorithms were built on ideas that largely fell into three different families of mathematical approaches.

"Of the 15 that made the cut, 12 are from these three families, with the remaining three algorithms based on other approaches," Moody said. "It's important for the eventual standard to offer multiple avenues to encryption, in case somebody manages to break one of them down the road."

Cryptographic algorithms protect information in many ways, for example by creating digital signatures that certify an electronic document's authenticity. The new standard will specify one or more quantum-resistant algorithms each for digital signatures, public-key encryption and the generation of cryptographic keys, augmenting those in FIPS 186-4, Special Publication (SP) 800-56A Revision 3 and SP 800-56B Revision 2, respectively.

For this third round, the organizers have taken the novel step of dividing the remaining candidate algorithms into two groups they call tracks. The first track contains the seven algorithms that appear to have the most promise.

"We're calling these seven the finalists," Moody said. "For the most part, they're general-purpose algorithms that we think could find wide application and be ready to go after the third round."

The eight alternate algorithms in the second track are those that either might need more time to mature or are tailored to more specific applications. The review process will continue after the third round ends, and eventually some of these second-track candidates could become part of the standard. Because all of the candidates still in play are essentially

survivors from the initial group of submissions from 2016, there will also be future consideration of more recently developed ideas, Moody said.

"The likely outcome is that at the end of this third round, we will standardize one or two algorithms for encryption and key establishment, and one or two others for digital signatures," he said. "But by the time we are finished, the review process will have been going on for five or six years, and someone may have had a good idea in the interim. So we'll find a way to look at newer approaches too."

Because of potential delays due to the COVID-19 pandemic, the third round has a looser schedule than past rounds. Moody said the review period will last about a year, after which NIST will issue a deadline to return comments for a few months afterward. Following this roughly 18-month period, NIST will plan to release the initial standard for quantum-resistant cryptography in 2022.

More information: Dustin Moody et al, Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, (2020). DOI: 10.6028/NIST.IR.8309

Provided by National Institute of Standards and Technology