NIST PQC Standards Next Steps

August 24, 2019

pqc-comments@nist.gov

What happens at the end of round 2?

- Hard decision to pick a subset of the candidates
  - The 20+ candidates in round 2 are quite good, and quite diverse
  - Based on what we know, none of them is obviously “the best choice”

- What can we do in the next 2-3 years that will help us decide?

Think about requirements & use cases	Analyze the candidate schemes
Which requirements are the most important? Where can we make compromises?	We can’t check everything, or test everything What are the key things that we need to analyze carefully?

Some of your responses to our survey

- The need for thorough analysis; don’t rush this
  - “Don’t rush and do this thing right. There is significant need for more analysis; many candidates have received relatively little substantive cryptanalysis…”
  - “Also, once the field has narrowed, there will be truly significant effort to make sure that implementations and validation procedures are sufficiently robust. Many of these algorithms are significantly more difficult to correctly implement than current primitives…”
  - “Attempting to end this process in just a couple more years is dangerous and could lead to disastrous results and/or a loss of perceived legitimacy of the process and output.”

Some of your responses to our survey

- Keep the focus on cryptanalysis in round 2
  - “Performance of schemes should not be a factor in Round 2, or at most a very minimal factor…. Security is what matters, and also maybe size.”
  - “But even those with optimized code, we are primarily measuring the Keccak within the implementation [and not the cost of the public key crypto].”
  - “Now is the time to reconsider if the parameters of the contest are correct, for example, do we need to protect against using 2^64 signatures?”

Some of your responses to our survey

- Keep the focus on cryptanalysis in round 2
  - “Organize a series of workshops focused on each class of post quantum algorithms (Lattice, Code Based, Multivariate, Hash based etc) … [to discuss] cryptanalysis in each area.”
  - “NIST needs to sponsor academic research at Universities across the United States in developing the science of quantum cryptanalysis.”

Some of your responses to our survey

- Improving the NIST process
  - “Integration of the os vendors, smart card vendors, piv card users to write the business requirements for pqc. We need to have more than cryptographic criteria documented for the selection.”
  - “Open a liaison with the Chinese Association for Cryptographic Research (CACR) to coordinate development of post quantum cryptographic standards…. The CACR algorithm competition recently posted 38 public key algorithms that were submitted to its competition….”

Some of your responses to our survey

- Improving the NIST process
  - “For the sake of transparency, NIST need to provide more insight into what will happen in the process. We hear there will be a Round 3, there will not be a Round 3. If NIST needs to put something together quickly, Adi Shamir recommended to select one or two mature algorithms to put out more quickly. Will NIST do this? Will there be more time for other schemes?”
  - “We see vastly different levels of maturity in security analysis. Adi Shamir’s suggestion to stream candidates into a regular bucket and a future bucket is an elegant solution.”

Some of your responses to our survey

- The need for outreach, to convince users to deploy PQC
  - “decommissioning old algorithms is difficult and … NIST [should assist] the commercial suppliers that are working to convince their end users of the need to upgrade”
  - “once standard primitives are established, … get them into relying application protocols (through the IETF, OASIS, ANSI, etc.), implemented and deployed as quickly as possible”

Some of your responses to our survey

- Community and outreach
    - “Ensure civility on the mailing list. Certain vocal and at times outright impolite personalities dominate the mailing list, causing others to hesitate to contribute their work or questions…”

Some of your responses to our survey

- PQC research topics
  - “NIST should devote some effort to developing migration plans that would allow new algorithm breakthroughs to be adopted as standards if warranted, possibly well before the expected 20 year lifespan of the 2022 standard comes to an end”
  - “There are a lot of lattice KEMs. Bernstein’s plan to systematically verify proofs should be followed. Otherwise there’s a risk of carrying proof errors and making decisions on a winner without fair comparison.”

Some of your responses to our survey

- The quantum threat
    - “Collect available data on quantum computing progress and assess when a quantum computer big enough to break a 2048-bit RSA key running Shors algorithm could be created.”
    - “NIST needs to use its resources to create estimates on when the real threat to existing public key cryptography will emerge… [because] the costs of switching out existing infrastructure will be huge.”

Some of your responses to our survey

- Should we slow down?

  - “NIST should not be aiming to conclude the process and have standards written by 2022. This is simply too fast to get proper answers…. Much more research is needed.”

  - “NIST should hold off creating any standard before 2025 and fund research efforts to look at all the candidates until that time. The process to date has provided the basis for a number of years of research. It is time to give researchers a chance to innovate.”

Wrap up

- Other questions or concerns? The survey is still open…
- Thank you for your participation, and have a safe trip home!

- What can we do in the next 2-3 years that will help us decide?

Think about requirements & use cases	Analyze the candidate schemes
Which requirements are the most important? Where can we make compromises?	We can’t check everything, or test everything What are the key things that we need to analyze carefully?