Public Comments Received on
NISTIR 8105 – Draft Report on Post-Quantum Cryptography
Public Comment Period Ended: March 9, 2016
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

As providers of custom cryptographic solutions for smartcards, DRM, car-to-car security, and other resource-constrained environments, we are especially familiar with long deployment timeframes and long equipment lifecycles. We support NIST's urgency in developing post-quantum replacements well before there is an actual threat to fielded solutions.

Based on preliminary evaluations, we are most interested in Ring Learning with Errors (RLWE) schemes and hash-based signature schemes, both stateful and stateless. Both types of schemes admit security proofs relating their hardness to well-defined mathematical problems. While setting parameter sizes for RLWE is less clear than for hash-based systems, we are encouraged by the level of scrutiny RLWE systems are currently receiving, in part due to their usage in advanced cryptographic constructions such as fully homomorphic encryption. We believe focusing on RLWE schemes is likely to have a great benefit beyond traditional security services like confidentiality and authenticity.

Current academic research has demonstrated that post-quantum algorithms can be integrated into widely-used protocols such as TLS. We hope to see more implementations addressing IKE, SSH, and the adoption of X.509 public key and signature formats. The security community will benefit from multiple approaches and implementations since the lessons learned for public protocols will guide efforts for custom and proprietary implementations. Finally, since we are often concerned with physical security of devices, we would like to see more consideration of side-channel attacks and whitebox obfuscation applied to post-quantum schemes.

John Wade, Cryptographer
Envieta Systems

>>>

To whom it may concern:

I would like to bring to your attention an additional class of Quantum Resistant algorithms for inclusion in Section Two of the Report on Post-Quantum Cryptography, those based on Group Theoretic Cryptography (GTC). GTC starts with the mathematics of Group Theory, which are usually non-abelian, infinite groups, and applies hard problems in those group theoretic areas to construct cryptographic algorithms. C.f. *Group Theoretic Cryptography*, Maria Isabel González Vasco, Rainer Steinwandt, April, 2015, Chapman and Hall/CRC, ISBN 9781584888369.

An example of GTC is the Algebraic Eraser (AE) suite of algorithms, which includes AEDH Key Agreement, AEDSA Signature, AEHash, and the AEBlock Cipher. All of the AE algorithms are rooted in various hard problems in an infinite, non-abelian braid group and based on a one-way function called E-Multiplication which is both rapidly computable and erases the data required for reversal. There are also other Group Theoretic algorithms in the public literature which may also be quantum resistant.

Shor's algorithm has made cryptographic protocols whose security is based on the hardness of computing discrete logarithms vulnerable to quantum attacks. Shor's algorithm has been further generalized to a larger set of hard problems now collectively known as the Hidden Subgroup Problem (HSP). The HSP has now been shown to be solvable on a quantum computer when the hidden subgroup is finite abelian or is one of a small class of finite non-abelian groups. The braid group used in the AE's E-Multiplication function does not contain any non-trivial finite subgroups at all, making it a viable quantum-resistant candidate for cryptography.

I believe you should specifically include this class of algorithms in your list in section 2, page 4.

Sincerely,

Derek Atkins

CTO SecureRF

>>>

Ludovic Perret

(Université Pierre et Marie Curie)

I am writing you regard the document « Report on Post-Quantum Cryptography » which provides a reasonable view of the current state-of-the art of post-quantum cryptography. Of course, I am happy that NIST is taking a position to push the community forward on the transition.

I have one question regarding the last part of the document :

> "While this process will have many commonalities with the processes that led to the standardization of AES [20] and SHA3 [21], this is not a competition. NIST sees its role as managing a process of achieving community consensus in a transparent and timely manner. Ideally, several algorithms will emerge as "good choices". NIST may pick one or more of these for standardization in each category. In this respect, NIST's process for standardizing quantum resistant public key cryptography will be similar to the ongoing block cipher modes development process [22]. "

I am not sure, but is the « ongoing block cipher modes development process » is referring to the CAESAR competition http://competitions.cr.yp.to/index.html ?

So, are you expecting that academics somewhat organize the selection process ?

>>>

Hildegard Ferraiolo (NIST)

Table 1 depicts the “Impact of Quantum Computing on Common Cryptographic Algorithms” showing impacts on signature, encryption, hashing functions, and key exchange. There is no impact on ‘authentication’. Authentication, however, is the front door to many off the “functions outlined in table 1.

Please consider authentication as one of the rows in table 1.

I recommend that the statement (and especially the bolded statement):

It is critical to engage with the community for NIST cryptographic standards to be endorsed by industry and other standards organizations around the world. **This Internal Report shares NIST’s current understanding about the status of quantum computing and post-quantum cryptography. The Report also outlines our initial plan to move forward.**

Recommendation:

NIST IR’s goal (as highlighted in bold) should take more prominence and be introduced earlier in the document.

>>>

Michael Harris (CDC)

Please expand on "crypto agility" and concrete things agencies/users can do to maintain it.

- Possible examples:

  (1) Migrate to stronger symmetric encryption and hashing now. Give detail on necessary configurations (e.g. key sizes, specific algorithms).

  (2) Avoid getting locked in to any specific crypto implementations (include flexibility in policies, planning, processes, procedures, procurement, and technology) and become ready and able to rapidly swap things in and out.

  (3) As early as 2023, it may be necessary to budget for some very significant retrofitting of entire security infrastructure if quantum computing has advanced enough that a rapid rather than gradual response is necessitated (could discuss scope of what needs to be considered for this planning).

>>>

David Hook (Crypto Workshop LLC)

I would like to suggest something to consider during the transition phase while new algorithms for post-quantum cryptography are being chosen.

At the moment there is a reasonable body of research supporting the security of key exchange methods based around Ring-learning-with-errrors (Ring-LWE). If my understanding is correct an algorithm implementing Ring-LWE should be disabled (as should any other non-approved algorithm) if a module which supports a Ring-LWE algorithm, such as NewHope, is running in FIPS approved mode.

I would like to suggest as an interim measure that the restriction requiring the disablement of these algorithms be relaxed if they are only used for the purpose of calculating material to go in the SuppPrivInfo component of the OtherInfo data described in Section

5.8.1.2 of SP 800-56A Revision 2. This condition could be outlined in the guidance section of the module's security policy.

At the worst this will not weaken the regular key agreement algorithms, at best, assuming no new research shows up suggesting Ring-LWE techniques are somehow flawed, it will have the effect of "post-quantum hardening" the key agreement calculations, as in addition to the regular key agreement value, another input to the KDF will be the key exchange value calculated using the Ring-LWE algorithm.

I think allowing this relaxation will also stimulate a lot of use and investigation into these algorithms as well, in a variety of ways. They do seem to be very different beasts to what we are used to dealing with, and in this case, where the use of them should do no harm, it would be worth providing some encouragement to allow their use in "real world"

applications. Choosing candidates for quantum-resistant cryptography is one thing, having good ways of applying the candidates is quite another.

[1] https://cryptojedi.org/papers/newhope-20151207.pdf "Post-quantum key exchange – a new hope", Alkim, Ducas, et al.

>>

David Jao (University of Waterloo)

My name is David Jao. I am the designer of post-quantum cryptosystems based on the isogeny problem over supersingular elliptic curves.

I was pleased to see that isogeny-based cryptosystems are included in the overview of post-quantum cryptosystems on page 4 of NIST IR 8105. On that page, you state regarding isogeny-based cryptosystems that "there has not been enough analysis to have much confidence in their security."

While I certainly agree with this statement, I hope that you will disclose the eventual criteria that you use to determine whether or not a system has had enough analysis. In particular, you also state on page 5 of NIST IR 8105 that "more research and analysis are needed before any of the above proposed post-quantum cryptosystems could be recommended for use today." This second statement implies that all of the main families of post-quantum primitives in your overview suffer from a lack of analysis, raising the question of why exactly isogeny-based cryptosystems are any worse than the others in this aspect. I hope that, in the final decision, uniform and published criteria will be applied to the evaluation of the proposals. Of course, there may exist objective criteria (such as date of earliest publication) which would favor one family over another. I emphasize here only the need for transparency because past experience has shown that NIST is at its best when the selection process is open and publicly visible.

On page 4 of the report, you state: "One challenge that will likely need to be overcome is that most of the quantum resistant algorithms have larger key sizes than the algorithms they will replace." I think it is important to emphasize just how important the key size constraint really is, and I would like to see key size considerations represented adequately in your eventual evaluation criteria. Many of the authors of NIST IR 8105 attended Dan Bernstein's talk at PQCrypto 2016 in which he discussed the network packet size (MTU) limits that are hard-coded into today's internet protocols. Most extant IPv4 hardware can only handle single network packets of a maximum size of 1500 bytes. For IPv6, the practical limit is 1280 maximum bytes in a single packet. Changing these limits is nearly impossible since it would require wholesale replacement of all existing internet hardware as well as making an incompatible change to fundamental internet protocols. Cryptography software in a malicious environment often must operate under the assumption that a public key must fit entirely in a single network packet, because multiple packets are too easy for an attacker to manipulate. Current protocols such as TLS and Tor are built with this assumption in mind. After accounting for protocol overhead, there are very few post-quantum primitives available today that can fit an entire public key into a single network packet at the 128-bit security level, and almost none that can do so at the 256-bit security level. You may find it interesting that recent work of myself and others (https://eprint.iacr.org/2016/229), to appear in AsiaPKC 2016, shows that isogeny public keys can fit into 384 bytes at the 128-bit security level and 768 bytes at the 256-bit security level. These numbers outperform every other post-quantum cryptographic primitive in the literature, even though our key size estimates are based entirely on quantum cryptanalysis whereas several of our closest competitors in this metric (such as QC-MDPC codes) admit to date only published estimates based on classical cryptanalysis.

The entire research community as well as the business sector is grateful to NIST for providing this forum to showcase the latest progress in post-quantum cryptography. It is wonderful to see NIST being proactive instead of reactive on this extremely critical issue.

>>

Morgan Stern (National Security Agency)

Page 1, paragraph beginning "In 1994..."

-Suggest adding a citation to Shor's paper here.

*Page 2, Table 1

-Possibly replace “AES-256” with “AES” so it is clear that "Larger key sizes needed" does not refer to creating an AES-512. This is assuming people are pretty comfortable with 256 since the later parts of the paper imply this table is targeting 128 bits of security.

-Similar to above, suggest changing SHA-256 to SHA-2 so "Larger output needed" sounds more like a recommendation to use the larger output sizes.

Page 5, first sentence

-At PQ Crypto 2016, comments were made to the effect that hash-based signatures may be standardized sooner than others. Possibly a comment to that effect could be made here.

Page 5, paragraph beginning "Over the years..."

-Suggest adding a reference to support saying "hundreds of thousands" because Reference 11 says it takes 500 million physical qubits (48:58) (or not, since [11] is specifically referring to factoring).

Page 6, paragraph beginning "It is useful..."

-Reference 14 doesn’t contain dollar amounts (as its location implies), just processor years.

Page 6 footnote

-Is this Moore's Law being defined as doubling every 18 months and a present-day cost of $250K to $30M to break 80 bits? (that is how I reproduce the figure of $1 billion in 30-40 years) Possibly include more details on the calculation, or a reference.

*Page 6, paragraph beginning "Previous..."

-I don't know if it is quite right that you are measuring "time complexity." If brute force search is parallelized among many computers it is just as much work (calls to the encryption algorithm for AES, say) but a lot less time. The phrase elsewhere in the paragraph that the "resources required to brute force search for a 128-bit cryptographic key" seems the more accurate phrase.

*Page 6, paragraph beginning "Unfortunately..."

- Reference 17 can be taken as supporting the earlier argument that doubling key size is very conservative. Reference 17 argues that because no quantum attack does better than square-root the time of a classical attack, but some do worse, the best classical attack isn't necessarily the best quantum. They make no claims (and have no examples) of a block cipher where a subexhaustive quantum attack exists but a classical attack does not. They have examples where the best quantum attack is less than a quadratic speedup of the best classical.

Page 6, paragraph beginning "Thus..."

-There are several users of NIST standards who likely will want higher than 128 bits of security. Note, for instance, NSA's CNSA Suite and the former Suite B for Top Secret both aim at a much higher level, so anyone hoping to serve the National Security market would want higher. Possibly there should be some recognition that some users will need higher security. Alternatively this may be an apples-to-oranges discussion once the concept of "quantum-security" is better defined.

-Note it is difficult to define n bits of quantum security as just the amount of quantum work required for Grover’s algorithm to recover a 2n-bit symmetric key. The main issue is that unstructured search is not the best approach to most post-quantum systems. So (for instance) the 128-bit quantum secure McElliece may have a much shorter lifetime than the 128-bit quantum secure AES256, not due to quantum attack, but because the classical attack on McElliece won't be much more than the quantum.

Page 7, paragraph beginning "When..."

-Do you have any advice for those who want to transition sooner than 10 years? In the CNSA Suite FAQ it is mentioned that for users with long intelligence life "one can use symmetric key cryptography in many instances to provide a measure of quantum resistance." You could include similar language in your document.

Some very minor editorial comments omitted