From: Chen, Lily (Fed)
To: Moody, Dustin (Fed); Liu, Yi-Kai (Fed); Perlner, Ray A. (Fed); Peralta, Rene C. (Fed); Daniel Smith (b) (6)
Subject: SC27 study period on quantum computing resistant cryptography
Date: Tuesday, May 3, 2016 8:51:00 AM
Attachments: v2-WG2 Nxxxx DRAFT Meeting report on WG2 SP QuantumApril2016.docx
v2_QCRC- Call for contributions-May2016.docx

This is an FYI. Attached are the summary of the previous study period and call for submissions of next study period.

Lily

DRAFT SC 27/WG 2 Nxxxx

DRAFT Rapporteur's Report on the Study Period on Quantum Computing Resistant Cryptography

1. Introduction

A Call for contributions was circulated based on the recommendation passed at the SC 27/WG 2 meeting held in Jaipur, India (see WG2 N1190). Six sets of comments were received in response to this Call for contributions (See WG2 N1212). A summary of the responses to the questions in the call for contributions is provided below.

a) Are you aware of any quantum computing resistant cryptographic algorithm/mechanism, which is publicly available? (e. g. hash-based signature XMSS)

In the responses, each contribution highlighted some quantum resistant cryptographic algorithm/mechanism, which was either published in the research literature and/or developed in the standards organizations such as IETF, ETSI, etc. Some contribution also mentioned the industry adoptions.

b) In your opinion, are any of the algorithms/mechanisms ready for ISO/IEC SC27 to standardize?

The following algorithms/mechanisms were considered as “ready” by different contributions for ISO/IEC SC27 to standardize.

- NTRU [1] [2]
- McEliece with binary Goppa codes using length n = 6960, dimension k = 5413 and adding t = 119 errors.
- Hash-based signatures
  - XMSS [3] with any of the parameters specified in [4].
  - SPHINCS-256 [5]
  - LMS [6]
- pqNTRUsign [7]

The following algorithms/mechanisms were considered as second phase selections for standardization.

- Quasi-cyclic MDPC codes [8] for McEliece with parameters at least n = 216 +6, k = 215 +3, d = 274 and adding t = 264 errors.

- The Stehlé–Steinfeld version [9] of the NTRU [2] lattice-based cryptosystem.
- The HFEv- [10] multivariate-quadratic signature system

c) In your opinion, which of the cryptographic functions shall be considered first? Key establishment, encryption, signature?

Five of the six responses recommended that signatures should be considered for standardization first, among which four contributions recommended that encryption or key establishment should also be considered for standardization at the same stage. One contribution recommended that KEM should be standardized first.

d) Other issues?

Two contributions point out the results on quantum cryptanalysis on symmetric-key based encryption schemes. One contribution points to a recent article published at http://eprint.iacr.org/2015/1018.pdf about moving forward to standardizing quantum computing resistant cryptography schemes without specifying a particular issue.

2. Discussions at the SC27 Tampa Meeting

At the Tampa meeting, the discussion focused on three major aspects.

The first is about how to consider the opinions presented by the received contributions. In particular, the maturity of the quantum computing resistant algorithms is not consistent with the urgencies of standardization. For example, hash-based signatures are relatively mature for their well-understood security assumptions. However, for backward secrecy, the encryption and key establishment functions may need to be standardized first. Some of the responses are based on the matureness while the others may consider backward secrecy.

The second aspect is how to introduce quantum computing resistant cryptography standards in SC27. One opinion is to add quantum computing resistant algorithms to the existing standards. For example, add quantum computing resistant encryption algorithms to ISO/IEC 18033-2 as an amendment. The reason is that quantum computing resistant algorithms shall satisfy the requirements for the existing standards and there is no need to define the new requirement. Another opinion is to define all the quantum computing resistant algorithms to a new standard series to specify quantum computing resistant encryption, signature, and key establishment mechanisms in different parts as it has been done for elliptic curve cryptography algorithms. These mechanisms could then later be moved to corresponding standards. Because quantum computing resistant cryptography is a new category, it may be easier to look into each specific desired function and create a separate standard for each type of mechanism.

The third aspect is how to move forward in SC 27. It was agreed that it may be more efficient to look into the specific algorithms. (See section 3 for agreed next step).

3. Next Step

It was agreed at the Tampa meetings to extend the study period for another six months. A new Call for contributions will be drafted to solicit further input on the algorithms responded to question b) in the previous call for contributions. In particular, the call for contributions will ask questions about whether the current requirements for public key encryption, digital signatures and key establishment are sufficient and proper for quantum computing resistant cryptography algorithms, whether new requirements are needed, and what they are if needed.

4. References

[1] IEEE P1363.1 “Public-Key Cryptographic Techniques Based on Hard Problems over Lattices” 2008

[2] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings, volume 1423 of Lecture Notes in Computer Science, pages 267–288. Springer, 1998.

[3] Johannes A. Buchmann, Erik Dahmen, and Andreas H¨ulsing. XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In Bo-Yin Yang, editor, Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings, volume 7071 of Lecture Notes in Computer Science, pages 117–129. Springer, 2011.

[4] Andreas Hülsing, Denis Butin, Stefan Gazdag, and Aziz Mohaisen. XMSS: Extended Hash-Based Signatures. Crypto Forum Research Group Internet-Draft, 2016.https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/

[5] Daniel J. Bernstein, Daira Hopwood, Andreas H¨ulsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O’Hearn. SPHINCS: Practical Stateless Hash-Based Signatures. In Elisabeth Oswald and Marc Fischlin, editors, Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria,

April 26-30, 2015, Proceedings, Part I, volume 9056 of Lecture Notes in Computer Science, pages 368–397. Springer, 2015.

[6] D. McGrew and M. Curcio "Hash-Based Signatures" https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/

[7] Jeff Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William Whyte. Transcript Secure Signatures Based on Modular Lattices. In Michele Mosca, editor, Post-Quantum Cryptography, number 8772 in Lecture Notes in Computer Science, pages 142{159. Springer International Publishing, October 2014

[8] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. In Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, 2013, pages 2069–2073. IEEE, 2013.

[9] Damien Stehlé and Ron Steinfeld. Making NTRU as Secure as Worst-Case Problems over Ideal Lattices. In Kenneth G. Paterson, editor, Advances in Cryptology – EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings, volume 6632 of Lecture Notes in Computer Science, pages 27–47. Springer, 2011.

[10] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In Ueli M. Maurer, editor, Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding, volume 1070 of Lecture Notes in Computer Science, pages 33–48. Springer, 1996.

SC 27/WG 2 N1265

Call for Contributions to SC 27/WG 2 Study Period on Quantum Computing Resistant Cryptography

(a.k.a. Post quantum cryptography (PQC), Quantum-safe cryptography (QSC))

This call for contributions is circulated in accordance with the recommendation passed at the SC 27/WG 2 meeting held in Tampa, Florida, USA on 11th – 15th April 2016 as an extension of the study period started in October 2015. Experts of National Bodies and Liaison Organizations of SC 27 are kindly asked to provide input to this study period.

The rapporteur appreciates all contributions regarding the status of quantum computing resistant cryptography algorithms and mechanisms. In particular, the study period seeks responses to the following questions.

a) In your opinion, which of the approaches shall SC 27 take in standardizing quantum computing resistant cryptography?
   1) Create a new standard series specifying quantum computing resistant cryptography in different parts, i.e. encryption, key establishment, and signature mechanisms would each be a unique part of the standard series; or
   2) Specify quantum computing resistant cryptography algorithms as amendments of existing standards.

b) Are there any additional or new security requirements that SC 27 should consider for quantum computing resistant cryptography besides the requirements and criteria used for selecting mechanisms for existing standards?

c) In your opinion, which of the following algorithms are ready to be standardized by SC 27 and why? Which of the following shall not be standardized and why? Are there additional algorithms not on this list that are ready to be standardized by SC 27 and why?

   - NTRU [1] [2]
   - McEliece with binary Goppa codes using length n = 6960, dimension k = 5413 and adding t = 119 errors.
   - Hash-based signatures
     - XMSS [3] with any of the parameters specified in [4].
     - SPHINCS-256 [5]
     - LMS [6]
   - pqNTRUsign [7]
   - Quasi-cyclic MDPC codes [8] for McEliece with parameters at least n = 216 +6, k = 215 +3, d = 274 and adding t = 264 errors.

- The Stehlé–Steinfeld version [9] of the NTRU [2] lattice-based cryptosystem.
- The HFEv- [10] multivariate-quadratic signature system

References

[1] IEEE P1363.1 “Public-Key Cryptographic Techniques Based on Hard Problems over Lattices” 2008

[2] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings, volume 1423 of Lecture Notes in Computer Science, pages 267–288. Springer, 1998.

[3] Johannes A. Buchmann, Erik Dahmen, and Andreas H¨ulsing. XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In Bo-Yin Yang, editor, Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings, volume 7071 of Lecture Notes in Computer Science, pages 117–129. Springer, 2011.

[4] Andreas Hülsing, Denis Butin, Stefan Gazdag, and Aziz Mohaisen. XMSS: Extended Hash-Based Signatures. Crypto Forum Research Group Internet-Draft, 2016.https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/

[5] Daniel J. Bernstein, Daira Hopwood, Andreas H¨ulsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O’Hearn. SPHINCS: Practical Stateless Hash-Based Signatures. In Elisabeth Oswald and Marc Fischlin, editors, Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I, volume 9056 of Lecture Notes in Computer Science, pages 368–397. Springer, 2015.

[6] D. McGrew and M. Curcio “Hash-Based Signatures” https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/

[7] Jeff Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William Whyte. Transcript Secure Signatures Based on Modular Lattices. In Michele Mosca, editor, Post-Quantum Cryptography, number 8772 in Lecture Notes in Computer Science, pages 142{159. Springer International Publishing, October 2014

[8] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. In Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, 2013, pages 2069–2073. IEEE, 2013.

[9] Damien Stehlé and Ron Steinfeld. Making NTRU as Secure as Worst-Case Problems over Ideal Lattices. In Kenneth G. Paterson, editor, Advances in Cryptology – EUROCRYPT 2011 - 30th Annual International Conference on

the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings, volume 6632 of Lecture Notes in Computer Science, pages 27–47. Springer, 2011.

[10] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In Ueli M. Maurer, editor, Advances in Cryptology - EUROCRYPT ’96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding, volume 1070 of Lecture Notes in Computer Science, pages 33–48. Springer, 1996.