The Transition from Classical to Post-Quantum Cryptography
draft-hoffman-c2pq-07

Abstract

   Quantum computing is the study of computers that use quantum features
   in calculations. For over 20 years, it has been known that if very
   large, specialized quantum computers could be built, they could have
   a devastating effect on asymmetric classical cryptographic algorithms
   such as RSA and elliptic curve signatures and key exchange, as well
   as (but in smaller scale) on symmetric cryptographic algorithms such
   as block ciphers, MACs, and hash functions. There has already been a
   great deal of study on how to create algorithms that will resist
   large, specialized quantum computers, but so far, the properties of
   those algorithms make them onerous to adopt before they are needed.

   Small quantum computers are being built today, but it is still far
   from clear when large, specialized quantum computers will be built
   that can recover private or secret keys in classical algorithms at
   the key sizes commonly used today. It is important to be able to
   predict when large, specialized quantum computers usable for
   cryptanalysis will be possible so that organization can change to
   post-quantum cryptographic algorithms well before they are needed.

   This document describes quantum computing, how it might be used to
   attack classical cryptographic algorithms, and possibly how to
   predict when large, specialized quantum computers will become
   feasible.

Status of This Memo

time. It is inappropriate to use Internet-Drafts as reference
material or to cite them other than as "work in progress."

This Internet-Draft will expire on November 27, 2020.

Copyright Notice

Table of Contents

1. Introduction

Early drafts of this document use "@@@@@" to indicate where the
editor particularly want input from reviewers. The editor welcomes
all types of review, but the areas marked with "@@@@@" are in the
most noticeable need of new material. (The editor particularly
appreciates new material that comes with references that can be
included in this document as well.)

1.1. Disclaimer

**** This is still an early version of this draft. **** As such, it
has had only some review in the cryptography community. Statements
in this document might be wrong; given that the entire document is
about cryptography, those wrong statements might have significant
security problems associated with them.

Readers of this document should not rely on any statements in this
version of this draft. As the draft gets more input from the
cryptography community over time, this disclaimer will be softened
and eventually eliminated.

1.2. Executive Summary

The development of quantum computers that can recover private or
secret keys in classical algorithms at the key sizes commonly used
today is at a very early stage. None of the published examples of
such quantum computers is useful in recovering keys that are in use
today. There is a great amount of interest in this development, and
researchers expect large strides in this development in the coming
decade.

There is active research in standardizing signing and key exchange
algorithms that will withstand attacks from large, specialized
quantum computers. However, all those algorithms to date have very
large keys, very large signatures, or both. Thus, there is a large
sustained cost in using those algorithms. Similarly, there is a
large cost in being surprised about when quantum computers can cause
damage to current cryptographic keys and signatures.

Because the world does not know when large, specialized quantum
computers that can recover cryptographic keys will be available,
organizations should be watching this area so that they have plenty
of time to either change to larger key sizes for classical
cryptography or to change to post-quantum algorithms. See Section 6
for a fuller discussion of determining how to predict when quantum
computers that can harm current cryptography might become feasible.

1.3. Terminology

The term "classical cryptography" is used to indicate the
cryptographic algorithms that are in common use today. In
particular, signature and key exchange algorithms that are based on
the difficulty of factoring numbers into two large prime numbers, or
are based on the difficulty of determining the discrete log of a
large composite number, are considered classical cryptography.

The term "post-quantum cryptography" refers to the invention and
study of cryptographic mechanisms in which the security does not rely
on computationally hard problems that can be efficiently solved on
quantum computers. This excludes systems whose security relies on
factoring numbers, or the difficulty of determining the discrete log
of one group element with respect to another.

Note that these definitions apply to only one aspect of quantum
computing as it relates to cryptography. It is expected that quantum
computing will also be able to be used against symmetric key
cryptography to make it possible to search for a secret symmetric key
using far fewer operations than are needed using classical computers
(see Section 5 for more detail). However, using longer keys to
thwart that possibility is not normally called "post-quantum
cryptography".

There are many terms that are only used in the field of quantum
computing, such as "qubit", "quantum algorithm", and so on. Chapter
1 of [NielsenChuang] has good definitions of such terms.

Some papers discussing quantum computers and cryptanalysis say that
large, specialized quantum computers "break" algorithms in classical
cryptography. This paper does not use that terminology because the
algorithms' strength will be reduced when large, specialized quantum
computers exist, but not to the point where there is an immediate
need to change algorithms.

The "^" symbol is used to indicate "the power of". The term "log"
always means "logarithm base 2".

1.4. Where to Read More

There are many reasonably accessible articles on Wikipedia, notably
the overview article at <https://en.wikipedia.org/wiki/
Quantum_computing> and the timeline of quantum computing developments
at <https://en.wikipedia.org/wiki/Timeline_of_quantum_computing>.

[NielsenChuang] is a well-regarded college textbook on quantum
computers. Prerequisites for understanding the book include linear
algebra and some quantum physics; however, even without those, a
reader can probably get value from the introductory material in the
book.

A good overview of the current status of quantum computing in general
is [ProgressProspects].

[QCPolicy] describes how the development of quantum computing affects
encryption policies.

[Turing50Youtube] is a good overview of the near-term and longer-term
prospects for designing and building quantum computers; it is a video
of a panel discussion by quantum hardware and software experts given
at the ACM's Turing 50 lecture.

@@@@@ Maybe add more references that might be useful to non-experts.

1.5. Not Covered: Post-Quantum Cryptographic Algorithms

This document discusses when an organization would want to consider
using post-quantum cryptographic algorithms, but definitely does not
delve into which of those algorithms would be best to use. Post-
quantum cryptography is an active field of research; in fact, it is
much more active than the study of when we might want to transition
from classical to post-quantum cryptography.

Readers interested in post-quantum cryptographic algorithms will have
no problem finding many articles proposing such algorithms, comparing
the many current proposals, and so on. An excellent starting point
is the web site <http://pqcrypto.org/>. The Open Quantum Safe (OQS)
project <https://openquantumsafe.org/> is developing and prototyping
quantum-resistant cryptography. Another is the article on post-
quantum cryptography at Wikipedia: <https://en.wikipedia.org/wiki/
Post-quantum_cryptography>.

Various organizations are working on standardizing the algorithms for
post-quantum cryptography. For example, the US National Institute of
Standards and Technology (commonly just called "NIST") is holding a
competition to evaluate post-quantum cryptographic algorithms.

NIST's description of that effort is currently at
<http://csrc.nist.gov/groups/ST/post-quantum-crypto/>. Until
recently, ETSI (the European Telecommunications Standards Institute)
had a Quantum-Safe Cryptography (QSC) Industry Specification Group
(ISG) that worked on specifying post-quantum algorithms; see
<http://www.etsi.org/technologies-clusters/technologies/quantum-safe-
cryptography> for results from this work.

1.6. Not Covered: Quantum Key Exchange

Other than in this section, this document does not cover "quantum key
exchange", also called "quantum cryptography". The field of quantum
key exchange uses quantum effects in order to secure communication
between users. Quantum key exchange is not related to cryptanalysis.

2. Brief Introduction to Quantum Computers

A quantum computer is a computer that uses quantum bits (qubits) in
quantum circuits to perform calculations. Quantum computers also use
classical bits and regular circuits: most calculations in a quantum
computer are a mix of classical and quantum bits and circuits. For
example, classical bits could be used for error correction or
controlling the behavior of physical components of the quantum
computer.

A basic principle that makes it possible to speed up calculations on
qubits in quantum computers is quantum superposition. Informally,
similarly to waves in classical physics, arbitrary number of quantum
states can be added together and result will be another valid quantum
state. That means that, for example, two qubits could be in any
quantum superposition of four states, three qubits in quantum
superposition of eight states, and so on. Generally n qubits can be
in quantum superposition of 2^n states.

The main challenge for quantum computing is to create and maintain a
significantly large number of superposed qubits while performing
quantum computations. Physical components of quantum computers that
are non-ideal results in the destruction of qubit state over time;
this is the source of errors in quantum computation. See Section 3.1
for a description of how to overcome this problem.

A good description of different aspects of calculations on quantum
computer could be found in [EstimatingPreimage].

A separate question is a measurement of a quantum state. Due to
uncertainty of the state, the measurement process is stochastic.
That means that in order to get the correct measurement one should
run several consequent calculations and corresponding measurement in

order to the expected value which is considered as a result of measurement.

@@@@@ Discuss measurements and how they have to be done with correlated qubits.

2.1. Quantum Computers that Recover Cryptographic Keys

Quantum computers are expected to be useful in the future for some problems that take up too many resources on a large classical computer. However, this document only discusses how they might recover cryptographic keys faster than classical computers. In order to recover cryptographic keys, a quantum computer needs to have a quantum circuit specifically designed for the type of key it is attempting to recover.

A quantum computer will need to have a circuit with thousands of qubits to be useful to recover the type and size keys that are in common use today. Smaller quantum computers (those with fewer qubits in superposition) are not useful for using Shor's algorithm (as discussed in Section 4.1) at all. That is, no one has devised a way to combine a bunch of smaller quantum computers to perform the same attacks on cryptographic keys via Shor's algorithm as a properly-sized quantum computer.

This is why this document uses the term "large, specialized quantum computer" when describing ones that can recover keys: there will certainly be small quantum computers built first, but those computers cannot recover the type and size keys that are in common use today. Further, there are already quantum computers that have many qubits but without the circuits needed to make those qubits useful for recovering cryptographic keys.

A straight-forward application of Shor's algorithm may not be the only way for large, specialized quantum computers to attack RSA keys. [LowResource] describes how to combine quantum computers with classical methods for recovering RSA keys at speeds faster than just using the classical methods.

3. Physical Designs for Quantum Computers

Quantum computers can be built using many different physical technologies. Deciding which physical technologies are best to pursue is an extremely active research topic. A few physical technologies (particularly trapped ions and neutral atoms, super-conduction using Josephson junctions, and nuclear magnetic resonance) are currently getting the most press, but other technologies are also showing promise.

One factor that is important to quantum computers that can be used for cryptanalysis is the speed of the operations (transformations) on qubits. Most of the estimates of speeds of these quantum computers assume that qubit operations will take about the same amount of time as operations in circuits that consist of classical gates and classical memory. Current quantum circuits are currently slower than classical circuits, but will certainly become faster as quantum computers are developed in the future.

Note that some current quantum computer research uses bits that are not fully entangled, and this will greatly affect their ability to make useful quantum calculations.

3.1. Qubits, Error Detection, and Error Correction

Researchers building small quantum computers have discovered that calculating the superposition of qubits often has a large rate of error, and that error rate increases rapidly over time. Performing quantum calculations such as those needed to recover cryptographic keys is not feasible with the current state of quantum computers.

In the future, actual quantum calculations will be performed on "logical qubits", that is, after the application of error correction codes on physical qubits. Thus, the number of physical qubits will be higher than the number of logical qubits, depending on the parameters of the error correction code, which in turn depends on the parameters of a technology used for a physical implementation of qubits. Currently, it is estimated that it takes hundreds or thousands of physical qubits to make a logical qubit. @@@@@ Need reference for this statement.

@@@@@ Lots more material should go here. We will need recent references for how many physical qubits are needed for each corrected qubit. It's OK if this section has lots of references, but hopefully they don't contradict each other.

3.2. Promising Physical Designs for Quantum Computers

@@@@@ It would be useful to have maybe two paragraphs about each physical design that is being actively pursued.

3.3. Challenges for Physical Designs

Different designs have different challenges to overcome before the physical technology can be scaled enough to build a useful large, specialized quantum computer. Some of those challenges include the following. (Note that some items on this list apply only to some of the physical technologies.)

Temperature: Getting stable operation without extreme cooling is
   difficult for many of the proposed technologies. The definition
   of "extreme" is different for different low-temperature
   technologies.

Stabilization: The length of time every qubit in a circuit holds is
   value

Quantum control: Coherence and reproducibility of qubits

Error detection and correction: Getting accurate results through
   simultaneous detection of bit-flip and phase-flip. See
   Section 3.1 for a longer description of this.

Substrate: The material on which the qubit circuits are built. This
   has a large effect on the stability of the qubits.

Particles: The atoms or sub-atomic particles used to make the qubits

Scalability: The ability to handle the number of physical qubits
   needed for the desired the circuit

Architecture: Ability to change quantum gates in a circuit

4. Quantum Computers and Public Key Cryptography

The area of quantum computing that has generated the most interest in
the cryptographic community is the ability of quantum computers to
find the private keys in encryption and signature algorithms based on
discrete logarithms using exponentially fewer operations than
classical computers would need to use.

As described in [RFC3766], it is widely believed that factoring large
numbers and finding discrete logs using classical computers increases
with the exponential size of the key. [RFC3766] describes in detail
how classical computers can be used to determine keys; even though
that RFC is over a decade old, no significant changes have been made
to the process of classical attacks on RSA and Diffie-Hellman. @@@@@
CFRG: is that true? Does RFC 3766 need to be updated?

Shor's algorithm shows that these problems can be solved on quantum
computers in polynomial time, meaning that the speed of finding the
keys is a polynomial function (with reasonable-sized coefficients)
based on the size of the keys, which would require significantly
fewer steps than a classical computer. The definitive paper on
Shor's algorithm is [Shor97].

4.1. Explanation of Shor's Algorithm

   @@@@@ Pointers to understandable articles would be good here.

   @@@@@ Describe period-finding and why it applies to finding prime
   factors and discrete logs.

   @@@@@ Give the steps for applying Shor's algorithm to 2048-bit RSA.
   Describe how many rounds of the quantum subroutine would likely be
   needed. Describe how many rounds of the classical loop would likely
   be needed.

   [ResourceElliptic] gives concrete estimates of the resources needed
   to build a quantum computer to compute elliptic curve discrete
   logarithms. It shows that for the common P-256 elliptic curve, 2330
   logical qubits and over 10^11 Toffoli gates.

   [PrimeFactAnneal] describes a method of converting the integer
   factorization problem to one that can be executed on an adiabatic
   quantum computer. Adiabatic quantum computers are already available
   today, such as those from D-Wave Systems. Note that this method is
   not a way to run Shor's algorithm on an adiabatic quantum computer.

4.2. Properties of Large, Specialized Quantum Computers Needed for
Recovering RSA Public Keys

   Researchers have built small quantum computers that implement Shor's
   algorithm, factoring numbers with four or five bits. These are used
   to show that Shor's algorithm is possible to realize in actual
   hardware. (Note, however, that [PretendingFactor] indicates that
   these experiments may have taken shortcuts that prevent them from
   indicating real Shor designs.)

   @@@@@ References are needed here. Did they implement all of Shor's
   algorithm, including the looping logic in the classical part and the
   looping logic in the quantum part?

   According to [GidneyEkera], a quantum computer that can determine the
   private keys for 2048-bit RSA would require 20 million correlated
   qubits. The paper estimates a similar order of size for a quantum
   computer that could determine the private key for 256-bit elliptic
   curve algorithms.

5. Quantum Computers and Symmetric Key Cryptography

   Section 4 is about Shor's algorithm and compromises to public key
   cryptography. There is a second quantum computing algorithm,
   Grover's algorithm, that is often mentioned at the same time as

Shor's algorithm. With respect to cryptanalysis, however, Grover's
algorithm applies to tasks of finding a preimage, including tasks of
finding a secret key of a symmetric algorithm such as AES if there is
knowledge of plaintext-ciphertext pairs. The definitive paper on
Grover's algorithm is by Grover: [Grover96]. Grover later wrote a
more accessible paper about the algorithm in [QuantumSearch].

Grover's algorithm gives a way to search for keys to symmetric
algorithms in the square root of the time that a normal exhaustive
search would take. Thus, a large, specialized quantum computer that
implements Grover's algorithm could find a secret AES-128 key in
about 2^{64} steps instead of the 2^{128} steps that would be required
for a classical computer.

When it appears that it is feasible to build a large, specialized
quantum computer that can defeat a particular symmetric algorithm at
a particular key size, the proper response would be to use keys with
twice as many bits. That is, if one is using the AES-128 algorithm
and there is a concern that an adversary might be able to build a
large, specialized quantum computer that is designed to attack
AES-128 keys, move to an algorithm that has keys twice as long as
AES-128, namely AES-256 (the block size used is not significant
here).

By some estimates, large specialized quantum computers that implement
Grover's algorithm might be built before ones that implement Shor's
algorithm are. There are two primary reasons for this:

o Grover's algorithm is likely to be useful in areas other than
   cryptography. For example, a large, specialized quantum computer
   that implements Grover's algorithm might help create medicines by
   speeding up complex problems that involve how proteins fold. @@@@@
   Add more likely examples and references here.

o A large, specialized quantum computer that can recover AES-128
   keys will likely be much smaller (and thus easier to build) than
   one that implements Shor's algorithm for 256-bit elliptic curves
   or 2048-bit RSA/DSA keys.

There are arguments against the likelihood of building computers
using Grover's algorithm to break AES-128. As described in
[FindCollisions]:

o Breaking AES-128 with Grover's method could be infeasible due to
   inherent inefficiencies in the algorithm. For example, the
   overhead of the quantum operations in the algorithm might be huge
   when compared to non-quantum operations.

o Grover's algorithm has not been parallelized in a quantum
   computer, so the 2^64 steps must be done serially. Unless the
   speed of quantum computations become as fast as current classical
   computers, this will make doing all the calculations needed to
   break an AES-128 key take so long as to be infeasible.

5.1. Properties of Large, Specialized Quantum Computers Needed for Recovering Symmetric Keys

[ApplyingGrover] estimates that a quantum computer that can determine
the secret keys for AES-128 would require 2953 correlated qubits and
2.74 * 2^86 gates.

[GoverSDES] shows how to use Grover's algorithm to search for keys in
SDES, a simplifed version of the DES encryption algorithm.

5.2. Properties of Large, Specialized Quantum Computers for Computing Hash Collisions

@@@@@ More goes here. Also, discuss how Grover's algorithm does not
appear to be useful for computing preimages (or say how it might be
used).

6. Predicting When Useful Cryptographic Attacks Will Be Feasible

If quantum computers that perform useful cryptographic attacks can be
built in the future, many organizations will want to start using
post-quantum algorithms well before those computers can be built.
However, given how few implementations of such quantum computers
exist (even for tiny keys), it is impossible to predict with any
accuracy when quantum computers that perform useful cryptographic
attacks will be feasible.

The term "useful" above is relative to the value of the material
being protected by the cryptographic algorithm to the attacker. For
example, if the quantum computer attacking a particular key costs
US$100 billion to build, costs US$1 billion a year to run, and can
extract only one key a year, it is possibly useful to some
governments, but probably not useful for attacking the TLS key used
to protect a small mail server. On the other hand, if later a
similar computer costs US$1 billion to build, costs US$10 million a
year to run, and can extract ten keys a year, many more keys become
vulnerable.

[BeReady] gives a simple way to approach the calculation of when one
needs to deploy post-quantum algorithms. In short, if the sum of how
long you need your keys to be secure plus how long it takes to deploy
new algorithms is longer than the length of time it will take for an

attacker to create a large, specialized quantum computer and use it
against your keys, then you waited too long.

To date, few people have done systematic research that would give
estimates for when useful quantum-based cryptographic attacks might
be feasible, and at what cost. Without such research, it is easy to
make wild guesses but those are not of much value to people having to
decide when to start using post-quantum cryptography.

For example, in [NIST8105], NIST says "researchers working on
building a quantum computer have estimated that it is likely that a
quantum computer capable of recovering 2000-bit RSA in a matter of
hours could be built by 2030 for a budget of about a billion
dollars". However, the referenced link is to a YouTube video
[MariantoniYoutube] where the researcher, Matteo Mariantoni, says
"maybe you should not quote me on that". [NIST8105] gives no other
references for predictions on cost and availability of useful
cryptographic attacks with quantum computers.

6.1. Proposal: Public Measurements of Various Quantum Technologies

In order to get a rough idea of when useful cryptographic attacks
with quantum computers may be feasible, researchers creating such
computers can demonstrate them when they can recover keys an eighth
the size of those in common use. That is, given that 2048-bit RSA,
256-bit elliptic curve, and AES-128 are common today, when a research
team has a computer than can recover 256-bit RSA, 32-bit elliptic
curve, or AES-128 where only 16 bits are unknown, they should
demonstrate it.

Such a demonstration could easily be made fair with trusted
representatives from the cryptographic community using verifiable
means to pick the keys to recover, and verifying the time that it
takes to recover each key. It might be interesting to run the same
tests in classical computers at the same time to give perspective.

These demonstrations will have many benefits to those who have to
decide when post-quantum algorithms should be deployed in various
environments.

o Demonstrations will likely use designs that are considered most
   efficient. This in turn will cause greater focus research on
   choosing good design candidates.

o The results of the demonstrations will help focus on issues
   important to cryptanalysis, namely the cost of building the
   systems and the speed of breaking a single key.

o Competing demonstrations will reveal where different research
   teams have made different optimizations from well-known designs.

o Public demonstrations could expose designs that work only in
   limited cases that are uncommon in normal cryptographic practice.
   (For example, [PretendingFactor] claims that all current
   factorization experiments have taken advantage of using a
   classical computer that already knows the answer to design the
   quantum circuits.)

Note that this proposal would only give an idea of how public
progress is being made on quantum computers. Well-funded military
agencies (and possibly even criminal enterprises) could be way ahead
of the publicly-visible computers. No one should rely on just the
public measurements when deciding how safe their keys are against
quantum computers.

7. IANA Considerations

None, and thus this section can be removed at final publication.

8. Security Considerations

This entire document is about cryptography, and thus about security.

See Section 1.1 for an important disclaimer about this document and
security.

This document is meant to help the reader predict when to transition
from using classical cryptographic algorithms to post-quantum
algorithms. That decision is ultimately up to the reader, and must
be made not only based on predictions of how quantum computing is
progressing but also the value of every key that the user handles.
For example, a financial institution using TLS to protect its
customers' transactions will probably consider its keys more valuable
than a small online store, and will thus be likely to begin the
transition earlier.

9. Acknowledgements

The list here is meant to acknowledge input to this document. The
people listed here do not necessarily agree with ideas presented.

Many sections of text were contributed by Grigory Marshalko and
Stanislav Smyshlyaev.

Some of the ideas in this document come from Denis Butin, Philip
Lafrance, Hilarie Orman, and Tomofumi Okubo.

[10](). References

[10.1](). Normative References

[Grover96]
          Grover, L., "A fast quantum mechanical algorithm for
          database search", 1996,
          <https://arxiv.org/abs/quant-ph/9605043>.

[Shor97] Shor, P., "Polynomial-Time Algorithms for Prime
          Factorization and Discrete Logarithms on a Quantum
          Computer", 1997,
          <http://epubs.siam.org/doi/pdf/10.1137/S0097539795293172>.

[10.2](). Informative References

[ApplyingGrover]
          Grassl, M., Langenberg, B., Roetteler, M., and R.
          Steinwandt, "Applying Grover's algorithm to AES: quantum
          resource estimates", 2015,
          <https://arxiv.org/abs/1512.04965>.

[BeReady] Mosca, M., "Cybersecurity in an era with quantum
          computers: will we be ready?", 2015,
          <http://eprint.iacr.org/2015/1075>.

[EstimatingPreimage]
          Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent,
          A., and J. Schanck, "Estimating the cost of generic
          quantum pre-image attacks on SHA-2 and SHA-3", 2016,
          <https://eprint.iacr.org/2016/992>.

[FindCollisions]
          Bernstein, D., "Quantum algorithms to find collisions",
          2017, <https://blog.cr.yp.to/20171017-collisions.html>.

[GidneyEkera]
          Gidney, C. and M. Ekera, "How to factor 2048 bit RSA
          integers in 8 hours using 20 million noisy qubits", 2019,
          <https://arxiv.org/abs/1905.09749>.

[GoverSDES]
          Denisenko, D. and M. Nikitenkova, "Application of Grover's
          Quantum Algorithm for SDES Key Searching", 2018.

[LowResource]
          Bernstein, D., Fiassse, J., and M. Mosca, "A low-resource
          quantum factoring algorithm", 2017,
          <https://eprint.iacr.org/2017/352.pdf>.

[MariantoniYoutube]
          Mariantoni, M., "Building a Superconducting Quantum
          Computer", 2014,
          <https://www.youtube.com/watch?v=wWHAs--HA1c>.

[NielsenChuang]
          Nielsen, M. and I. Chuang, "Quantum Computation and
          Quantum Information, 10th Anniversary Edition", ISBN
          97801-107-00217-3 , 2010.

[NIST8105]
          Chen, L. and et. al, "Report on Post-Quantum
          Cryptography", 2016,
          <http://nvlpubs.nist.gov/nistpubs/ir/2016/
          NIST.IR.8105.pdf>.

[PretendingFactor]
          Smolin, J., Vargo, A., and J. Smolin, "Pretending to
          factor large numbers on a quantum computer", 2013,
          <https://arxiv.org/abs/1301.7007>.

[PrimeFactAnneal]
          Jiang, S., Britt, K., McCaskey, A., Humble, T., and S.
          Kais, "Quantum Annealing for Prime Factorization", 2018,
          <https://www.nature.com/articles/s41598-018-36058-z>.

[ProgressProspects]
          The National Acadamies Sciences Engineering Medicine,
          "Quantum Computing: Progress and Prospects (2019)", 2019,
          <https://www.nap.edu/catalog/25196/
          quantum-computing-progress-and-prospects>.

[QCPolicy]
          Princeton University Center for Information Technology
          Policy, "Implications of Quantum Computing for Encryption
          Policy", 2019, <https://carnegieendowment.org/2019/04/25/
          implications-of-quantum-computing-for-encryption-policy-
          pub-78985>.

[QuantumSearch]
          Grover, L., "From Schrodinger's Equation to the Quantum
          Search Algorithm", 2001,
          <https://arxiv.org/abs/quant-ph/0109116>.

   [ResourceElliptic]
              Roetteler, M., Naehrig, M., Svore, K., and K. Lauter,
              "Quantum Resource Estimates for Computing Elliptic Curve
              Discrete Logarithms", 2017,
              <https://eprint.iacr.org/2017/598>.

   [RFC3766] Orman, H. and P. Hoffman, "Determining Strengths For
              Public Keys Used For Exchanging Symmetric Keys", BCP 86,
              RFC 3766, DOI 10.17487/RFC3766, April 2004,
              <https://www.rfc-editor.org/info/rfc3766>.

   [Turing50Youtube]
              Vazirani, U., Aharonov, D., Gambetta, J., Martinis, J.,
              and A. Yao, "Quantum Computing: Far Away? Around the
              Corner?", 2017,
              <https://www.youtube.com/watch?v=SzfJRR5JrgQ>.

Author's Address

   Paul Hoffman
   ICANN

   Email: paul.hoffman@icann.org