Quantum Computing and the DNS

ICANN Office of the Chief Technology Officer

Paul Hoffman
OCTO-031
11 February 2022

TABLE OF CONTENTS

This document is part of ICANN's Office of the Chief Technical Officer (OCTO) document series. Please see the OCTO publication page for a list of documents in the series. If you have questions or suggestions on any of these documents, please send them to octo@icann.org.

This document supports ICANN's strategic goal to improve the shared responsibility for upholding the security and stability of the Domain Name System (DNS) by strengthening DNS coordination in partnership with relevant stakeholders. It is part of ICANN's strategic objective to strengthen the security of the DNS and the DNS root server system (RSS).

Executive Summary

Quantum computers have attracted the attention of the security community in recent years due to the possibility that they will be able to undermine currently-popular cryptographic algorithms. There are no quantum computers powerful enough to do so today, but as the technology slowly improves, there may come a day when some of the algorithms in use today will be easily broken by this new type of computer. However, because quantum computing technology is still new and building and running quantum computers is incredibly expensive, it is difficult to predict how long into the foreseeable future that day might come.

New algorithms that are assumed impervious to quantum computers are now being standardized. This paper examines recent work that makes better estimates for when the Domain Name System (DNS) community needs to consider changing from current cryptographic algorithms to new ones.

1 Introduction

Some algorithms in modern cryptography depend on the difficulty of certain math problems that take huge amounts of time to solve. Quantum computers might be able to solve these problems much faster, which would then weaken the assurances of those algorithms. Computers based on quantum principles are fundamentally different from the computers that have been widely used in the last 70 years. Data processing on quantum computers relies on quantum bits, called *qubits*, instead of the binary bits that all computers today use.

If large-scale quantum computers can be built, they might be able to solve some problems that are impossible with current computing technology because quantum computers can handle many complex processes at the same time. Even though today's computers, called *classical computers*, can handle parallel processes, quantum computers can do so using tighter connections between the parts of the data being analyzed.

The concepts behind quantum computers have been theorized for nearly 50 years, but it is phenomenally difficult to build even very small quantum computers. The information in qubits is quite fragile, so qubits must be completely isolated from the external environment by keeping them at temperatures near zero degrees Kelvin during computations; doing so takes a lot of machinery and physical space. However, qubits are also highly prone to errors during processing. A quantum computer needs hundreds or thousands of additional cooled qubits to correct errors for every qubit in the computation; and making a quantum computer with millions of qubits may be impossible due to the cooling and communication requirements.

1.1 Quantum Computers and Cryptography

If quantum computers of sufficient size can be built, they are expected to have applications in a few broad areas. A quantum computer is said to be of "sufficient size" if it can perform problems that cannot be performed by the largest classical computers. Such quantum computers will possibly be useful for physics research, for complex chemistry and biology problems, and for some complex business models; however, it is not clear that quantum computers, which are useful for these tasks, can even be built.

Another area where quantum computers might be used is to break cryptographic algorithms that are presumed to be impossible to break with classical computers. The two types of algorithms that are thought to be susceptible to future quantum computers are the RSA and Diffie-Hellman schemes (including elliptic curve Diffie-Hellman) for digital signatures and key exchange which are used nearly universally on the Internet today. (RSA and Diffie-Hellman schemes are also known mathematically as the hard problems of factoring and finding the discrete logarithms of large integers.)

A quantum computer that can break these schemes significantly faster than classical computers is called a "cryptographically relevant quantum computer," abbreviated as "CRQC." If CRQCs could be built, the security properties of all the common signature and key exchange algorithms in common use on the Internet today would be significantly weakened. Such a result would obviously be terrible: signatures using those algorithms could be forged and secrets that were protected by those key exchanges would be revealed.

To be able to break the RSA and Diffie-Hellman schemes when used with key sizes that are commonly in use currently, a CRQC would need to be incredibly large, much larger than any quantum computer that can be built today. Building small quantum computers is not good enough to break cryptography; one cannot just run a small quantum computer for longer in order to break the cryptographic keys, nor can one run a bunch of small quantum computers in parallel to achieve the task.

We must estimate when a CRQC can be built in order to estimate how soon we need to change to using "post-quantum cryptography" (abbreviated as "PQC") that will resist quantum computers. PQC algorithms are believed to not be susceptible to breakage by any quantum computer because they have fundamentally different properties from the RSA and Diffie-Hellman schemes.

2 Quantum Computers and Cryptography

Recently, three documents were published that look at the question of when the first CRQCs might be created. These documents are the basis for the analysis in this paper.

- *Internet Security and Quantum Computing,*[1] by Hilarie Orman, is an academic paper that describes the fundamentals of current quantum computing and cryptography. Many parts of the paper are accessible to normal technical readers, although many other parts will only make sense to readers with strong backgrounds in modern physics. Because there was a dearth of publications on this topic, ICANN financially sponsored the research and writing of the academic paper.
- *Landscape of Quantum Computing in 2021,*[2] by Sam Jaques, is an informal web site describing the current state of large-scale quantum computers. The site is centered around an excellent graph showing what has been created so far, and how far quantum computers need to evolve before they can even start to be useful as CRQCs.
- *Quantum Technology and Its Impact on Security in Mobile Networks,*[3] by John Preuß Mattsson, Ben Smeets, Erik Thormarker from Ericsson, is a report covering many

[1] See https://eprint.iacr.org/2021/1637
[2] See https://sam-jaques.appspot.com/quantum_landscape
[3] See https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/ensuring-security-in-mobile-networks-post-quantum

aspects of quantum technology and security. The report shows where future quantum computers will affect Internet security, with a focus on cellular wireless networks.

Readers interested in this topic should read, or at least skim, all three documents. The analysis in this document mostly relies on the analysis in the *Internet Security and Quantum Computing* paper and the *Landscape of Quantum Computing in 2021* web site. (Readers with a strong physics background who want a much more in-depth description of quantum computing might want to also read *Quantum Computation and Quantum Information, 10th Anniversary Edition*, a classic textbook on the topic.[4])

2.1 When To Be Concerned About Future Quantum Computers

The Internet Security and Quantum Computing paper and the Landscape of Quantum Computing in 2021 web site both come to the same conclusion about CRQCs. It is exceedingly unlikely that CRQCs will be built any time soon, certainly not in the next decade. Internet Security and Quantum Computing describes the immense engineering hurdles needed to build a quantum computer of any significant size over the next 50 years, and Landscape of Quantum Computing in 2021 shows graphically the large distance between what is possible today and where the world would need to be for a quantum computer to be useful.

This conclusion is useful in thinking about how to transition from RSA and Diffie-Hellman schemes to PQC algorithms. An attacker will inherently value the ability to forge signatures differently from learning secrets that were protected in key exchanges. Because of this difference, the need to change from RSA and Diffie-Hellman schemes to PQC is different for systems that use digital signatures and systems that use key exchange.

2.2 Post-Quantum Cryptography

Although signature and key exchange algorithms based on RSA and Diffie-Hellman schemes are susceptible to CRQCs, there are other types of algorithms that are believed not to be. The *Internet Security and Quantum Computing* paper describes how the private keys in RSA and Diffie-Hellman can be significantly weakened by a quantum computer that implements Shor's algorithm, a quantum computing algorithm that was described in 1994 by Peter Shor.[5] PQC algorithms, some of which are now only experimentally deployed, are those that are not weakened by Shor's algorithm.

Research in PQC has been active for many years, and some of the algorithms being discussed are decades old. The primary reason that PQC algorithms have not been widely deployed on the Internet before now is that they take significantly more computational work than ones based on RSA and Diffie-Hellman. Also, some PQC algorithms have extremely large keys and/or signature sizes, which can have effects on how well they can replace the currently-used

[4] "Quantum Computation and Quantum Information, 10th Anniversary Edition" by Michael Nielsen and Isaac Chuang, 2010, Cambridge University Press, ISBN 978-1-10700-217-3

[5] See https://www.youtube.com/watch?v=6qD9XElTpCE

algorithms in practice. ICANN's Security and Stability Advisory Committee has a report on the possible effects of these large keys and/or signatures on DNSSEC.[6]

There are many different proposals for PQC replacements for signatures and key exchange. They are being actively discussed in many places, most notably in the U.S. National Institute for Standards and Technology (NIST) Post-Quantum Cryptography Standardization Process[7] (often mistakenly called the NIST "competition"). The process is a multi-year, multi-round set of events coordinated by the NIST which will culminate in a set of standards for the U.S. government; these standards will likely be adopted by many other organizations as well. It is important to note that NIST is not alone in evaluating PQC algorithms, and it is likely that many different algorithms with different properties (such as different key sizes and different computational complexity) will be adopted in different communities.

3 Quantum Computers and DNSSEC

The signatures used throughout DNSSEC today are based on RSA and elliptic curve Diffie-Hellman. If CRQCs become available, an attacker with such a computer can determine the private keys associated with the public keys used in DNSSEC, and use those private keys to sign malicious DNSSEC records and fool validators about their authenticity.

There are two methods for the DNSSEC community to prevent CRQC attacks on DNSSEC: adopt larger RSA or elliptic curve Diffie-Hellman keys, or move to PQC signature algorithms. Moving to larger keys is an ineffective strategy because if the engineering and quantum technology becomes good enough to build a CRQC for today's key sizes, building one that is a few times larger is probably not that difficult. Thus, the DNSSEC community will need to move to PQC signature algorithms at least a few years before CRQCs become feasible and could be economically used in practice.

It is important to note that someone who possesses a CRQC will choose to use it in the most economical fashion. Early CRQCs will cost billions of dollars to build, and quite possibly cost billions of dollars to operate due to the high cost of keeping the qubits at temperatures near zero degrees kelvin. If the organization who owns the CRQC is an attacker (as compared to a research institution), the attacker will choose which keys are most economically beneficial to break. Being able to impersonate authoritative DNS servers by using stolen DNSSEC keys could be more valuable in the future when DNSSEC adoption is higher, although it is quite unclear what the value to an attacker would be to be able to do a short-term impersonation.

4 Quantum Computers and TLS

By far, most of the concern over CRQCs, however, is for keeping both short- and long-term secrets. Private information that is transmitted under Transport Layer Security (TLS) can be revealed by learning the keys used in the TLS key exchange, and essentially all of today's TLS implementations use RSA and Diffie-Hellman schemes for exchanging keys. If an attacker has kept copies of an entire set of messages including the TLS setup, they can read the content of the messages after determining the private key used.

[6] See https://www.icann.org/en/system/files/files/sac-107-en.pdf
[7] See https://csrc.nist.gov/projects/post-quantum-cryptography

The vast majority of TLS use today is for web traffic and other systems that rely on HTTP interactions. The DNS only uses TLS to a small extent, to make DNS traffic between some stub resolvers and recursive resolvers private. It does so using technologies such as DNS-over-TLS (RFC 7858, "Specification for DNS over TLS"[8]) and DNS-over-HTTPS (RFC 8484, "DNS Queries over HTTPS"[9]).

There are three methods for the TLS-using communities to prevent CRQC attacks on TLS: adopt larger RSA or Diffie-Hellman keys, include a pre-shared secret key (such as a strong password) in the key exchange, or move to PQC key exchange algorithms. Moving to larger keys is an ineffective strategy for the same reasons described in Section 3. Including a pre-shared secret key is impractical for general TLS use because the client and the server do not have any easy way to establish the pre-shared secret.

The TLS community is already actively discussing how to move to PQC key exchange algorithms. The primary reason for the desire to move as quickly as feasible is that some of the secrets that are being protected by TLS today could be valuable for 40 years, and thus be valuable to an attacker in the far future. Because it is impossible to determine how long it will take for CRQCs to be built, and because some people believe it can be done in time for some of today's secrets to still be valuable to attackers, switching to PQC key exchange algorithms soon will prevent attacks on future secrets.

5 ICANN Positions

Because the ICANN community has not developed a consensus on how developments in quantum computing relate to the DNS, any possible position of the ICANN organization regarding this matter lacks community input. However, as it relates to the secure and stable operation of the DNS, there are some basic principles on which ICANN's Office of the Chief Technology Officer does have an opinion and would like to share the following.

To be clear, the following principles are not intended to be prescriptive or identify areas in which ICANN has specific responsibilities. Rather, they aim to be supportive of efforts to ensure a single, stable, secure, and globally interoperable DNS by increasing the trust end users can place on the DNS.

5.1 The DNSSEC Community Does Not Need to Consider Post-Quantum Cryptography At This Time

Without massive and unexpected discoveries in both quantum physics and engineering for quantum computers, there is no chance that a cryptographically relevant quantum computer (CRQC) could be built in the next decade, and possibly not for many decades. Even after waiting a decade, there will clearly be years if not decades of warning before a CRQC will be built, and that amount of time will be more than sufficient for the DNSSEC community to adopt

[8] See https://datatracker.ietf.org/doc/rfc7858/
[9] See https://datatracker.ietf.org/doc/rfc8484/

one or more appropriate signature algorithms based on post-quantum cryptography (PQC). The expected timelines for the development of CRQCs are described in the *Internet Security and Quantum Computing* paper and the *Landscape of Quantum Computing in 2021* web site.

If the DNSSEC community waits until it is significantly clearer when a CRQC can be built, it becomes much more likely that the PQC signature algorithms chosen for the DNS will be a better fit for DNSSEC. The NIST process so far has focused on PQC key exchange algorithms because comparing the features of the proposed signature algorithms is much more difficult, and much less urgent. Taking the additional time will let the DNSSEC community hone their choices to those most appropriate to the DNS.

5.2 DNS Protocols That Also Use TLS Should Update to Post-Quantum Cryptography In Alignment with Web Protocols

The choice of PQC key agreement algorithms used in TLS should be unrelated to the choice of PQC signature algorithms used in DNSSEC. The damage that an attacker with a CRQC could do to privacy is likely much worse than the damage they can do to authentication. DNS's nascent use of TLS for communications privacy in DNS-over-TLS and DNS-over-HTTPS should have no effect on the TLS community's decision process for when to transition to PQC key exchange. When the TLS community selects PQC algorithms, the DNS community should follow the TLS community's choices for the parts of DNS that use TLS.