Quantum Computing and the DNS

ICANN Office of the Chief Technology Officer

Paul Hoffman

OCTO-031v2
22 April 2024

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).

This revision contains updates to reflect advances in quantum computing and post-quantum cryptography. ICANN appreciates the many suggestions made by the community on OCTO-031v1.

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 time 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 precisely when that day might come.

New algorithms that are assumed impervious to quantum computers are now being standardized. This paper examines recent work that provides 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 those 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 problems that are unsolvable 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.

While the concepts behind quantum computers have been theorized for nearly 50 years, it is extremely 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. Therefore, building 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 predicted 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.[1]

Another area in which 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 based on the mathematically 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 currently widely used, a CRQC would need to be extremely large, much larger than any quantum computer that can be built today. Building small quantum computers is not sufficient to break cryptography; one cannot just run a small quantum computer for a longer time to break the cryptographic keys, nor can one run many 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 considered to not be susceptible to breakage by any quantum computer because they have fundamentally different properties from the RSA and Diffie-Hellman schemes. (Some people have started using the term “quantum-ready” instead of “post-quantum”.)

2 Quantum Computers and Cryptography

2.1 Background

Because of the importance of determining when and if future attackers can break the cryptography on which the Internet relies, many papers and studies have been published, and many conferences and symposia have been held. Two documents about PCQ stand out, and are the basis for the analysis in this paper. (Readers with a strong physics background who want a much more in-depth description of quantum computing might also want to read *Quantum Computation and Quantum Information, 10th Anniversary Edition*, the classic textbook on the topic.[2])

[1] See https://spectrum.ieee.org/quantum-computing-skeptics

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

2.1.1 Internet Security and Quantum Computing

Internet Security and Quantum Computing,[3] by Hilarie Orman, is a 2021 academic paper that describes the fundamentals of quantum computing and cryptography. Many parts of the paper are accessible to regular technically inclined readers. However, some other parts will only make sense to readers with a strong background in modern physics.

2.1.2 Recent Progress in Quantum Computing Relevant to Internet Security

Recent Progress in Quantum Computing Relevant to Internet Security,[4] also by Hilarie Orman, covers advancements in quantum algorithms and computers after *Internet Security and Quantum Computing* was published. Many announcements related to the field have been made in the past few years. This paper provides a deep dive into both the usefulness of the technological advancements and their context with respect to Internet security. Because there exists a dearth of publications on this topic, ICANN financially sponsored the research and writing of the two academic papers.

2.1.3 Landscape of Quantum Computing

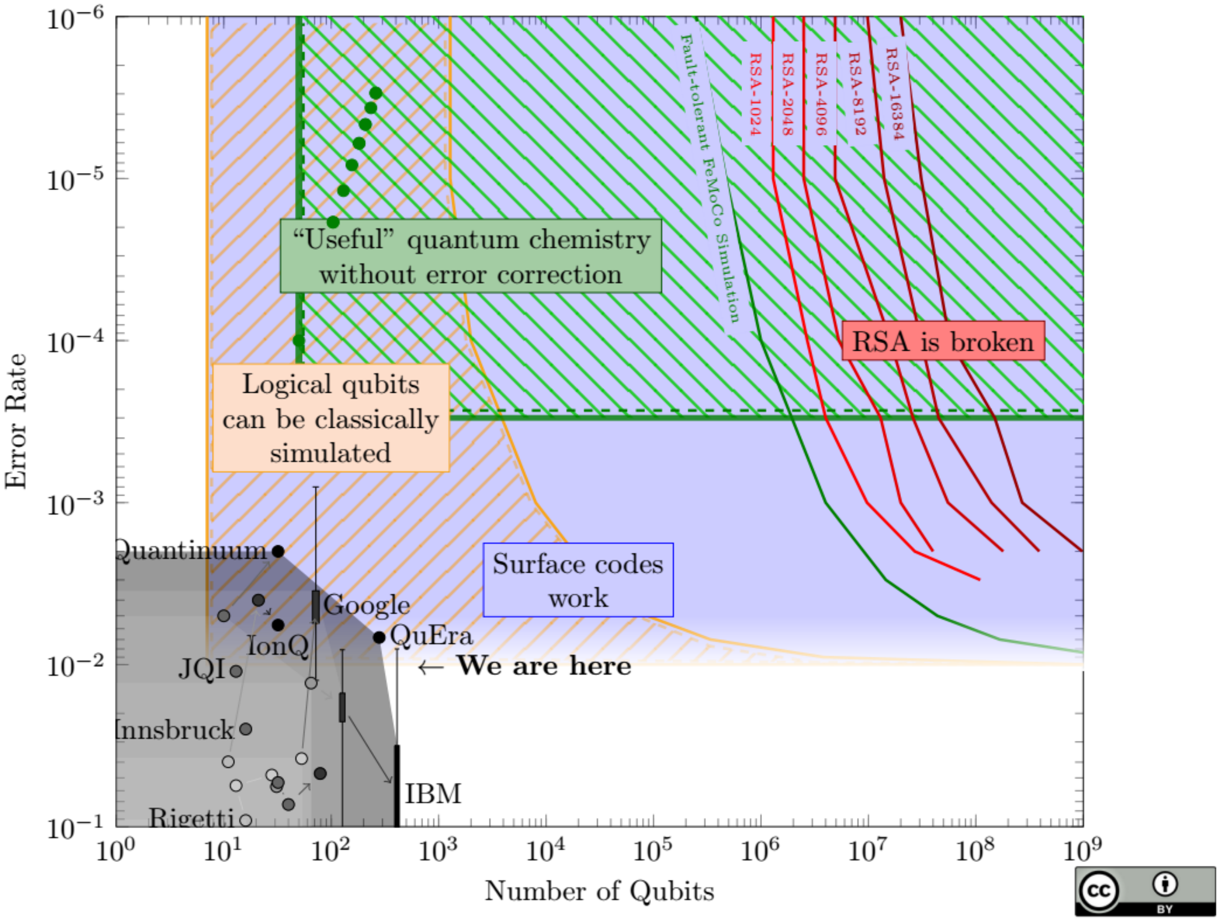
Landscape of Quantum Computing in 2023,[5] by Sam Jaques, is an informal web site describing the current state of large-scale quantum computers. The site is centered around an excellent graph showing what has been created so far, and how far quantum computers need to evolve before they can even start to be useful as CRQCs.

The site uses two charts based on the most recent reports to show how close the world is to having a quantum computer that can break RSA encryption with 1024-bit keys. The first chart shows the current state of quantum computing in the lower left, and the amount of quantum computing that would be needed to break RSA in the upper right; note that both the vertical and horizontal axes use logarithm scales.

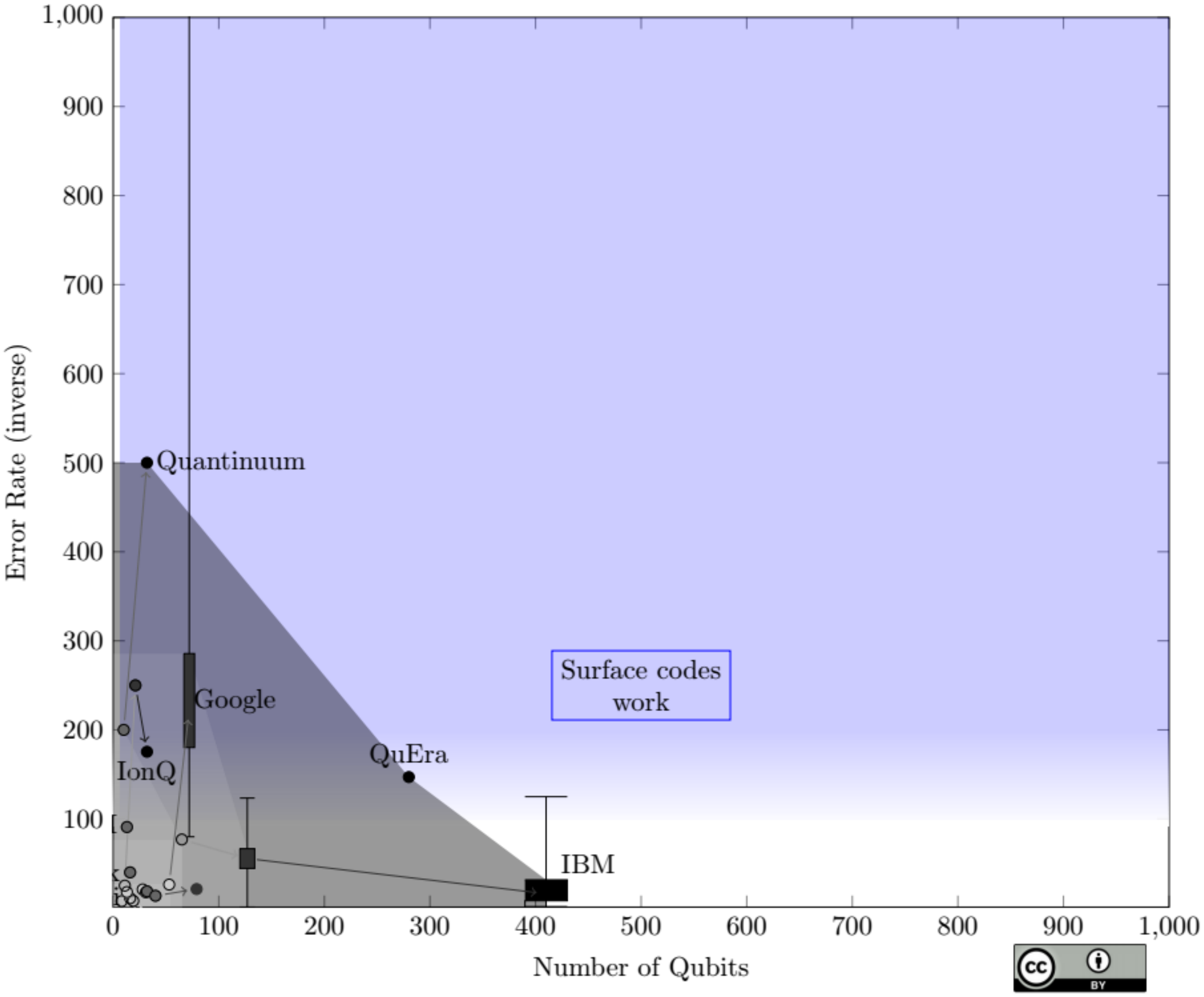
[3] See https://eprint.iacr.org/2021/1637

[4] See https://eprint.iacr.org/2024/410.pdf

[5] See Landscape of Quantum Computing © 2023 Sam Jaques, https://sam-jaques.appspot.com/quantum_landscape_2023



The second chart shows the same data as the first, but without using logarithm scales. As noted on the web site, "the distance from today's quantum computers to breaking RSA is about 10,000 chart-widths".



2.2 When To Be Concerned About Future Quantum Computers

The *Internet Security and Quantum Computing* and *Recent Progress in Quantum Computing Relevant to Internet Security* papers, and the *Landscape of Quantum Computing in 2023* web site, 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 2023* 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.

The Global Risk Institute and the quantum-focused cybersecurity company evolutionQ publish an annual report that synthesizes the views of dozens of experts in the field of quantum computers. Their *Quantum Threat Timeline Report 2023*[6] details the different perspectives and extrapolates them into various charts and tables. The report features experts in quantum computing, not in predicting the future. Therefore, the validity of the experts' previous predictions is not listed in the report. Further, the report's methodology assumes that all experts possess an equal ability to predict the future and thus can be combined equally, but this is not described in the report. Therefore, the summaries from the report are not based on the validity of predictions of the experts.

2.3 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.[7] 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 those based on RSA and Diffie-Hellman. Also, some PQC algorithms have extremely large keys and/or signature sizes, which can effect how well they can replace the currently used algorithms in practice. ICANN's Security and Stability Advisory Committee published a report on the possible effects of these large keys and/or signatures on Domain Name System Security Extensions (DNSSEC).[8]

Many different proposals for PQC replacements for signatures and key exchanges are being discussed in various forums, most notably in the U.S. National Institute for Standards and Technology (NIST) Post-Quantum Cryptography Standardization Process[9] (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 use by the U.S. government. These standards will likely be adopted by many other organizations. The first set of algorithms chosen by NIST for PQC signatures and key exchange was announced in 2023. The final standardization specifications for those algorithms are expected in 2024. NIST expects to announce additional PCQ signature and key exchange algorithms in 2026 and beyond.

It is important to note that NIST is not alone in evaluating PQC algorithms. 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. NIST has also said that it will later publish additional guidance for selecting key sizes for some of the signature algorithms.

[6] See https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/
[7] See https://www.youtube.com/watch?v=6qD9XElTpCE
[8] See https://www.icann.org/en/system/files/files/sac-107-en.pdf
[9] See https://csrc.nist.gov/projects/post-quantum-cryptography

The Internet Engineering Task Force (IETF) is already standardizing the use of PQC algorithms in Internet protocols, and its work is ongoing. This work is also happening in the Crypto Forum (CFRG)[10], which is part of the Internet Research Task force (IRTF). The IRTF is affiliated with the IETF. There are already RFCs for various PQC signatures, and active work on more PQC signatures and key encapsulation mechanisms (KEMs), mostly based on the NIST algorithms. IETF work on PQC algorithms is being tracked (but not managed) by the Post-Quantum Use In Protocols (pquip) Working Group.[11] The working group provides a lengthy page listing the various IETF PQC work.[12]

Some organizations are not yet prepared to fully trust new PQC algorithms, so they want to first transition to using both current and PQC algorithms at the same time. Combining more than one algorithm in this way creates a *hybrid* algorithm. Using hybrid algorithms takes more CPU time to sign, verify, or encrypt; it also causes more traffic because there are more keys. Some protocols, such as Messaging Layer Security (MLS)[13], require a hybrid key exchange, while others (such as TLS) make hybrid signatures and encryption optional.

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 them 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 against CRQCs 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. This transition must take place with enough time for most of the resolver and signing software and hardware to be updated.

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.

[10] See https://datatracker.ietf.org/group/cfrg/documents/
[11] See https://datatracker.ietf.org/group/pquip/documents/
[12] See https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc
[13] See https://datatracker.ietf.org/doc/rfc9420/

4 Quantum Computers and TLS

The biggest concern by far related to CRQCs, however, is 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 and QUIC key exchanges, and essentially all of today's TLS and QUIC 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.

The vast majority of encryption is currently used for web traffic and other systems that rely on HTTP interactions. The DNS only uses TLS and QUIC to a small extent: to make DNS traffic between some stub resolvers and recursive resolvers private. It does so by using technologies such as DNS-over-TLS (RFC 7858, "Specification for DNS over TLS"[14]), DNS-over-HTTPS (RFC 8484, "DNS Queries over HTTPS"[15]), and DNS-over-QUIC (RFC 9250, "DNS over Dedicated QUIC Connections"[16]).

Web communities can use three methods to prevent CRQC attacks on encrypted HTTP: 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 as described in Section 3. Including a pre-shared secret key is impractical for general web use because the client and the server do not have any easy way to establish the pre-shared secret.

The web community is already actively discussing how to move to PQC key exchange algorithms, using either PQC or hybrid algorithms. The primary reason for wanting to move as quickly as feasible is that some of the secrets that are being protected by TLS and QUIC 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 experts believe it can be done while some of today's secrets are still 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.

[14] See https://datatracker.ietf.org/doc/rfc7858/
[15] See https://datatracker.ietf.org/doc/rfc8484/
[16] See https://datatracker.ietf.org/doc/rfc9250/

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 beyond the next decade, there will be years if not decades of advanced notice before a CRQC will be built. This lead time will be more than sufficient for the DNSSEC community to adopt 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 2023* 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 or QUIC Should Update to Post-Quantum Cryptography in Alignment with Web Protocols

DNS’s nascent use of TLS and QUIC for communications privacy in DNS-over-TLS, DNS-over-HTTPS, and DNS-over-QUIC should have no effect on the web community’s decision process for when to transition to PQC key exchange. When the web community selects PQC algorithms for key exchange, the DNS community should follow that community’s choices for the parts of the DNS that use encryption.