PQC for DNSSEC: a format size analysis on Falcon signatures

Ginevra Fabrizio
University of Twente
Enschede, The Netherlands
g.fabrizio@utwente.nl

Ralph Koning
SIDN Labs and University of Amsterdam
Arnhem, The Netherlands
ralph.koning@sidn.nl

Elmer Lastdrager
SIDN Labs
Arnhem, The Netherlands
elmer.lastdrager@sidn.nl

Caspar Schutijser
SIDN Labs
Arnhem, The Netherlands
caspar.schutijser@sidn.nl

Anna Sperotto
University of Twente
Enschede, The Netherlands
a.sperotto@utwente.nl

Roland van Rijswijk-Deij
University of Twente
Enschede, The Netherlands
r.m.vanrijswijk@utwente.nl

ABSTRACT

Falcon is a post-quantum signature algorithm recently chosen for standardization by the National Institute of Standards and Technology (NIST). Its official implementation has two different signature formats that differ in size. In this paper, we measure the impact of the two different formats of Falcon signatures on DNSSEC-signed zones and on DNSSEC queries, based on real-world traffic for a large country-code Top Level Domain (ccTLD). We take into consideration Falcon's two signature formats, called padded and compressed, and evaluate their effects on DNSSEC signature sizes. We provide a signature size distribution for each format, using data obtained from a DNSSEC-signed ccTLD zone and queries for this zone. We use the results to study whether there are advantages to choosing one of the two signature formats. Our results show that the difference in DNS message size between padded and compressed signatures is small. Therefore, while in theory smaller signatures are favorable, the use of the compressed signature format does not have tangible real-world benefits. As our results show, the use of compressed signatures does not lead to a significant shift in message size such that more DNSSEC answers would fit within MTU limits. These results provide useful input for the discussion on Falcon signature standardization in DNSSEC, concluding that standardization of a fixed-size padded format may be preferable for its predictability and to avoid potential implementation errors.

Applied Networking Research Workshop (ANRW '25), July 22, 2025, Madrid, Spain, 2025.

CCS CONCEPTS

• **Networks** → **Application layer protocols**; • **Security and privacy** → *Network security*; **Digital signatures**.

KEYWORDS

Post-Quantum Cryptography, DNSSEC, Digital Signatures, Falcon

ACM Reference Format:
Ginevra Fabrizio, Ralph Koning, Elmer Lastdrager, Caspar Schutijser, Anna Sperotto, and Roland van Rijswijk-Deij. 2025. PQC for DNSSEC: a format size analysis on Falcon signatures. In *Applied Networking Research Workshop (ANRW '25), July 22, 2025, Madrid, Spain.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3744200.3744767

1 INTRODUCTION

Post-quantum cryptography (PQC) is essential to protect our telecommunication systems from the future arrival of quantum computers. Achieving complete post-quantum security is a complex transition process that has to be carried out by everyone in the Internet landscape, sooner or later. This process is of extreme importance as quantum computers are capable of breaking many current cryptographic algorithms. Eventually, all Internet protocols that make use of public key cryptography will have to switch to quantum-safe cryptography.

In this paper, we look at one protocol in particular, the Domain Name System's Security Extensions (DNSSEC). The DNS is a foundational component of the Internet as we know it, making translation from human-readable domain names (like `example.com`) into machine-readable IP addresses (like `91.198.174.192`) possible. DNSSEC adds vital security properties to the DNS by digitally signing DNS records, that allow recipients of DNS messages to validate the authenticity and integrity of DNS records. This process, that happens on a global scale every day, relies on public-key cryptography and can be quite easily broken by a quantum computer's computing capabilities.

To ensure widespread availability of quantum-safe cryptographic algorithms, the US National Institute of Standards and Technology (NIST), launched a competition to select post-quantum algorithms for standardization from candidates submitted by the cryptographic community. As of March 2025, 5 algorithms have been selected for standardization [4]. One of these candidates is Falcon [3], a signature scheme that is based on NTRU lattices [3]. Falcon is attracting attention because of its relatively efficient performance in terms of processing requirements, offering fast signing and verification times. Its key and signature sizes are also smaller and have a balanced size compared to most other post-quantum candidates. This makes it a likely candidate for use in DNSSEC [10], where these features are desirable.

Other aspects, such as CPU and memory usage, also relate to the impact of processing the DNSSEC messages at scale. The impact on these resources is indeed significant [12], but it is not the focus of this paper as our analysis focuses on the signature size distributions. Because of this, we want to evaluate Falcon's performance in real-world DNSSEC queries, by testing two out of its three different kinds of signature formats, compressed and padded. These two formats differ in how they handle signature sizes, the compressed format allows for the shortest signature size but has variable size, while the padded format has a fixed size, that is generally larger. The third format, CT, will not be considered in this paper, as it is intended to protect against timing side-channel attacks that do not apply to the DNSSEC use case.

The contributions of this work are that we:

(1) collect real-world data for a large DNSSEC-signed ccTLD, including the signed zone and one day of queries to this zone;
(2) use this data to simulate DNSSEC signing of this ccTLD with Falcon's two signature formats;
(3) show the real-world implications of choosing either signature format for DNSSEC operations.

The remainder of the paper is structured as follows. First, in §2 we briefly discuss background on Falcon and DNSSEC and provide related work on these two subjects. Then, we describe our approach in §3 and we detail our research results in §4. We finally conclude by discussing the impact of Falcon unpadded signatures on DNSSEC-signed zones in §5.

2 BACKGROUND AND RELATED WORK

In this section we first provide a background on DNSSEC and its post-quantum challenges. Next, we show related work on this topic.

2.1 DNS and DNSSEC

The DNS translates domain names to IP addresses, in a process called name resolution. However, DNS does not guarantee authenticity and integrity. So, to address these vulnerabilities in traditional DNS, DNSSEC was introduced. DNSSEC ensures the messages have not been tampered with through the use of digital signatures. DNSSEC uses public-key cryptography to sign DNS records. When a domain owner wants to ensure their domain's DNS records are secure, they sign those records with a private key. The corresponding public key is published in the DNS zone file. The public key is stored in a special DNS record called the `DNSKEY` record. This key is used by clients to verify that the DNS record they receive is authentic and has not been tampered with. DNSSEC also plays an important role in proving the non-existence of a DNS record. To achieve this, two record types are also signed, the `NSEC` (Next Secure) and `NSEC3` (Next Secure 3) records. These signatures, while essential for security, affect the size of DNS messages [13].

In a typical DNS response, only the so-called `ANSWER` section will contain signatures and any optional records in the `AUTHORITY` and `ADDITIONAL` sections are left out to keep DNSSEC-signed responses small [14]. In a delegation/referral, however, the `AUTHORITY` section will contain the delegation with the `DS` record and its signature. The additional section may include optional records with additional signatures, depending on the name server configuration. These signatures contribute to the overall size of the DNS message. For example, responses for nonexistent domains (`NXDOMAIN`) tend to be large precisely because they contain many signatures over `NSEC(3)` records. The presence of many signatures in a response, especially in the case of `NXDOMAIN` with multiple `NSEC(3)` records, can lead to large packets that exceed the maximum DNS message size limits.

2.2 Post-quantum impact on DNSSEC

Migrating to a post-quantum DNSSEC protocol has its own challenges, but the most critical one is the size of the signatures [7]. The transition process on its own does not pose particular challenges as DNSSEC is not new to rolling out new signing algorithms and this has already happened in the past [11]. However, these new algorithms must be compatible with the requirements already existing in DNS, DNSSEC and the underlying transport protocols.

Falcon has been announced to be standardized by NIST in the near future, together with 2 other signature scheme candidates (SPHINCS+[5] and Dilithium [6]). Falcon has been considered for use in DNSSEC as a post-quantum algorithm, as it offers a favorable balance between signature size and public key size, making it a viable candidate for DNSSEC applications [10].

Falcon's official implementation allows for three different kinds of signature formats [2]:

- **Compressed (unpadded) format**: the default signature format in Falcon. Its variable size offers the smallest signature sizes on average, making it efficient for storage and transmission purposes.
- **Padded format**: similar to the compressed format but with additional padding to achieve a fixed signature size. Ensures consistent signature size, for systems where a predictable signature size is necessary, such as in constrained environments.
- **Constant Time (CT) format**: designed to prevent timing side-channel attacks by ensuring constant-time operations. This mode has a fixed size signature, larger than both compressed and padded formats.

The CT format is considered irrelevant for DNSSEC as timing side-channel attacks generally do not apply to how signatures are used in DNSSEC. For this reason, the CT format will not be considered in this work. However, as holds for almost all post-quantum signature scheme algorithms, Falcon signatures are bigger compared to currently used signature schemes.Falcon-generated signatures contribute to the overall size of DNSSEC messages. For top-level domain zones, this includes signatures on `DS` (Delegation Signer) records in delegations, and signatures on `NSEC` or `NSEC3` records for authenticated denial of existence. In particular, responses for nonexistent domains (RCODE 3, `NXDOMAIN`) can include multiple `NSEC3` records, each with a signature, leading to potentially large packets. These potentially large messages pose a critical problem: overly large DNS messages pose a challenge to DNSSEC. They can exceed maximum message size limits imposed by DNS Flag Day [1], such as the MTU of 1,500 bytes or the 1,232 byte limit to stay within the minimum MTU of IPv6. When a message is too large to fit into a single datagram, it requires fragmentation into multiple packets or a fallback over the TCP protocol, affecting efficiency. The size of DNSSEC messages is already a problem and using bigger signatures, such as post-quantum ones, will only make the problem worse.

2.3 Related work

Previous work on `NXDOMAIN` response size distributions has been carried out in [14]. That work shows and explains the multi-peak pattern in `NXDOMAIN` response size distributions caused by the presence of multiple `NSEC3` records, demonstrating that there is valid concern surrounding DNSSEC message size. The issue of large signature size is an active area of research. For example, the IETF issued a draft on a "compact denial of existence" [9] that aims to reduce `NXDOMAIN` responses and DNSSEC messages size. The impact of PQC on DNSSEC has also been studied in previous work, including a theoretical analysis of the suitability of PQC algorithms for DNSSEC [10] and ways to transmit large DNSSEC responses due to large PQC signatures using novel approaches to fragmentation [8]. To the best of our knowledge, ours is the first work to actively measure the difference between Falcon signature formats applied to real-world DNSSEC records.

3 METHODOLOGY

To analyze the real-world impact of the different Falcon implementation options, we leverage real-world data from a large DNSSEC-signed country-code Top Level Domain (ccTLD), `.nl`. We create a version of the `.nl` zone file that we sign with Falcon in unpadded mode. We then replay one day of queries towards the `.nl` zone to record message sizes for Falcon in padded and in unpadded mode.

3.1 Data extraction and preprocessing

We collect all DNS queries from the network traffic for the authoritative name servers of the `.nl` zone in a 24-hour period using the ENTRADA system run by the `.nl` ccTLD. ENTRADA (ENhanced Top-level domain Resilience through Advanced Data Analysis) is a tool for analyzing very large volumes of DNS data[1]. It processes PCAPs from the `.nl` authoritative name servers, extracts data related to DNS traffic, annotates it, and stores it into a database that can be queried for analysis. We requested two data sets for a 24-hour period on April 3rd, 2025, one for DNS queries with a `NOERROR` (`RCODE=0`) response, and one for DNS queries with an `NXDOMAIN` (`RCODE=3`) response. All `NOERROR` responses from both valid and invalid subdomains are used.

We specifically select these two response codes as they are the most common responses returned by the ccTLD's authoritative name servers and they generally include one or more signatures (in `RRSIG` records). The first one, `NOERROR`, indicates that the authoritative name server successfully returned a response to the query, which in case of a ccTLD indicates a so-called referral to a delegation for one of the second-level domains registered in the ccTLD. In other words, assume we queried for `example.nl`, then a `NOERROR` response contains a referral to the name servers for that domain. In a DNSSEC-signed TLD, such a referral typically includes a *signed* `DS` record that binds the signing key for the delegated domain to the `DNSKEY` records of that domain. The second one, `NXDOMAIN`, indicates that the authoritative name server does not know the name queried for, which in case of a ccTLD indicates that the queried second-level domain does not exist. This response includes one or more *signed* `NSEC3` records that cryptographically prove that the domain really does not exist.

[1] https://entrada.sidnlabs.nl

The data sets (in CSV format), contain the queried domain name, the query type (qtype) and the number of queries with the specified RCODE that occurred during the 24-hour time period. Before replaying the queries we filtered out empty and clearly illegal queries using the following regular expression: `^[a-zA-Z0-9_-].\+,[0-9]\+,[0-9]\+$`. For illegal queries we mean queries that contain characters that are not allowed in domain names, such as '@' or other non-printable characters. The regular expression only filters queries that have illegal characters at the start of the query name. Any illegal characters later in the query (e.g., `example***.nl`) are not filtered out. This filtering removed 76 queries from the NOERROR data set and 20,332 from the NXDOMAIN data set. We filter for two main technical reasons: (i) parsing the original CSV caused 222 library parsing errors, and (ii) some other queries caused encoding parsing errors, so we could not load those domain names to execute the queries.

3.2 Zone signing and experimental setup

We took the zone file of .nl for the same day (April 3rd, 2025) and removed all existing DNSSEC data. The stripped zone is then signed twice with Falcon-512, creating two signed versions of the zone one using the padded and one using the unpadded format. Additionally, we had the signer add NSEC3 records for both zones. NSEC3 is used for authenticated denial of existence, each NSEC3 record is also signed. Depending on the query type, responses may include multiple signatures (RRSIG records).

Both Falcon-512 based zone files are hosted using NSD[2] on a virtual machine with 16 dedicated Xeon 5115 CPU cores and 125G of memory, with the padded version served on port 5331 and the unpadded version on port 5332.

3.3 Query replay and response capture

Each query recorded in the NOERROR and NXDOMAIN data set is replayed against both NSD instances and we record the RCODE and the size of the response message. Note that for each query we now have 3 RCODE values, one recorded by the ccTLD's collection system for the original query, one for the query against the NSD hosting the padded zone file, and one for the query against the unpadded zone file. Although, on paper each query should have the same RCODE, in practice we expect some discrepancies due to changes in the zone file over the 24-hour period that we collected query data for.

In Table 1 we see the responses we got from replaying the data. NOERROR, REFUSED, and NXDOMAIN are DNS response codes whereas ValueError and IndexError are runtime errors of the Python script that replays the queries. This only happens in the NXDOMAIN data set because this also contains failed queries containing nonsensical domain names and disallowed character sets that are rejected by the DNS. The Python-specific errors are excluded from further analysis since they do not include response sizes.

Response Code	NOERROR (RCODE=0)	NXDOMAIN (RCODE=3)
NOERROR	**59,312,128**	11,142
REFUSED	15,857	5,161
NXDOMAIN	12,357	**113,348,878**
ValueError	–	117
IndexError	–	14

Table 1: Number of NOERROR and NXDOMAIN responses

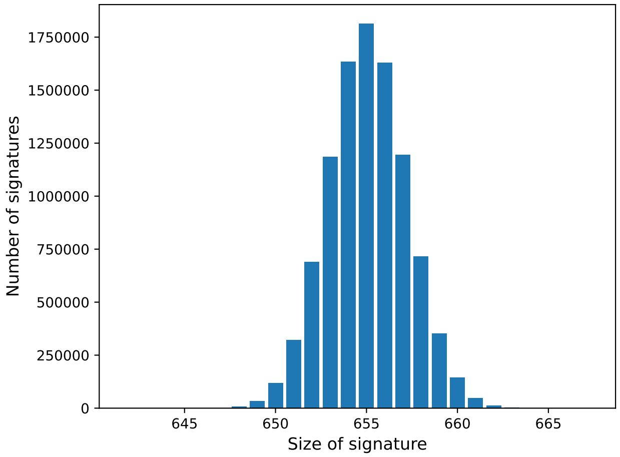

Figure 1: Signature size distribution for unpadded Falcon in the signed .nl zone file.

Through the message size measurement we can analyze the size distribution of the obtained messages, for both versions of the zone (padded and unpadded) and for both response codes (NOERROR and NXDOMAIN). The different size message distributions are then compared, to assess whether the use of non-padded signatures results in a higher frequency of smaller DNS messages compared to padded signatures. Particularly, we focus on the number of messages that exceed critical size thresholds, specifically **1,500 bytes** (the default MTU for Ethernet) and **1,232 bytes**, the recommended maximum DNS message size as per DNS Flag Day [1]. The goal is to determine whether non-padded signatures reduce the number of messages that exceed these thresholds, thereby avoiding fragmentation or a relatively costly fallback to TCP.

[2] NLnet Labs Name Server Daemon (NSD): https://www.nlnetlabs.nl/projects/nsd/about/

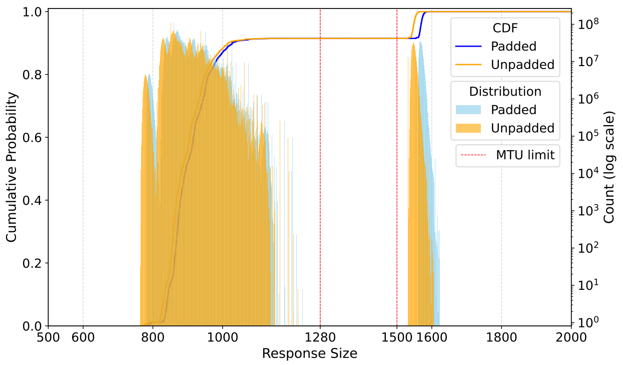

Figure 2: Cumulative distribution function of response size distribution (left axis) and histogram of number of responses of a specific size (right axis, log scale) over a day for Falcon DNSSEC responses for `NOERROR` responses in the `NOERROR` data set.

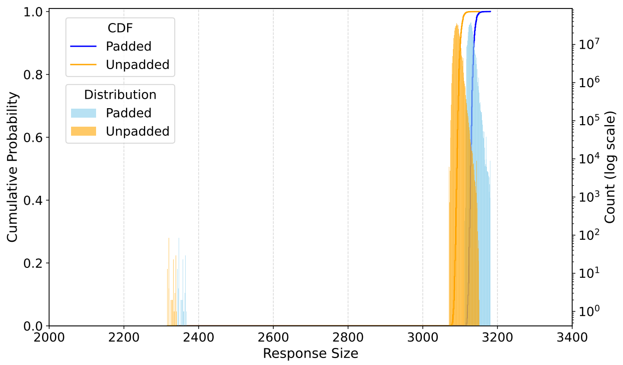

Figure 3: Cumulative distribution function of response size distribution (left axis) and histogram of number of responses of a specific size (right axis, log scale) over a day for Falcon DNSSEC responses for `NXDOMAIN` responses in the `NXDOMAIN` data set.

4 RESULTS

4.1 Signature size distribution

We start by analyzing the signature size distribution for unpadded Falcon-512 signatures for our `.nl` zone file. Figure 1 shows the signature size distribution. As the figure shows, the distribution is bell-shaped, with a median signature size of 655 bytes (compared to the fixed signature size of 666 bytes for padded Falcon-512). This distribution is consistent with the reference implementations for Falcon-512 [2]. While not visible in the plot, we note that unpadded Falcon-512 can actually produce signatures that are larger than the fixed padded signature size, and we observe one case of an unpadded signature with a size of 667 bytes in our test zone. The reason that padded signatures are always 666 bytes, despite larger signatures occurring in practice, is that the algorithm for the padded version will keep generating a new signature until its size is less than or equal to 666 bytes. While repeating signing operations impacts efficiency, the likelihood that this occurs in practice is very low. In our dataset with 9,912,711 signatures only a single signature is 667 bytes. As Figure 1 shows, the unpadded variant can produce signatures of different sizes, but generally speaking unpadded Falcon-512 produces smaller signatures than the padded variant.

4.2 Impact on real-world response sizes

We next turn to the impact on real-world response sizes. We first look at the differences for the `NOERROR` data set, where we focus on responses that also had `NOERROR` as response code when we replayed the queries against our test zones (top-left in Table 1, 59.3M responses). Figure 2 shows the CDF for the response size distribution (left axis) and a histogram of query counts for specific response sizes (right axis, log scale). As the figure shows, responses with padded (blue) and unpadded (orange) signatures for existing domain names only exhibit a minimal difference in message size. This difference is not meaningful enough to influence the number of responses that fit within the typical 1,500 or 1,232-byte response size limits. We can, however, clearly see that the majority of responses fit within these limits anyway. A smaller, but non-negligible fraction of responses, however, exceeds these size limits, and the size difference between responses with padded and unpadded signatures is also more pronounced here (right-hand side of the plot). Responses in this category contain an extra signature due to the inclusion of an `NSEC3` record that proves the non-existence of a `DS` record for the queried domain. In other words: the absence of DNSSEC-signing in the second-level domain that is queried for produces a larger result when querying the `.nl` zone that exceeds maximum message size limits if Falcon-512 is used for signing.

Next, we look at the differences between padded and unpadded signatures for the `NXDOMAIN` data set. In this case

Response size	Response code	Response behavior
<77*	`REFUSED` (5)*	empty response*
764–1,229	`NOERROR` (0)	the requested records
1,532–1,622	`NOERROR` (0)	1 signed `NSEC3` record
2,269–2,420	`NXDOMAIN` (3)	2 signed `NSEC3` records
3,075–3,767	`NXDOMAIN` (3)	3 signed `NSEC3` records

*Not shown in Figures 2 and 3.

Table 2: DNS response sizes clearly map to certain response behaviors

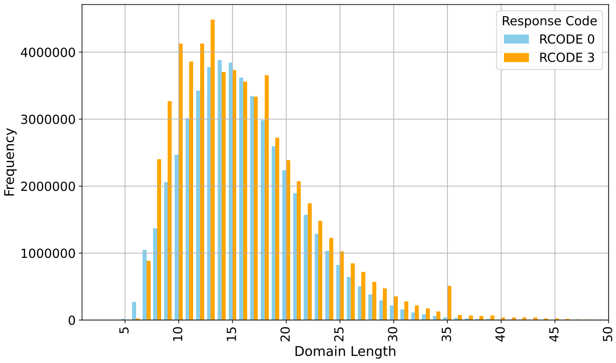

Figure 4: Domain length distribution for existing (NOERROR) and non-existing (NXDOMAIN) domains for a day of DNSSEC queries.

we focus on responses that also had NXDOMAIN as response code when we replayed the queries against our test zones (third row on the right in Table 1, 113.3M responses). Figure 3 again shows the CDF (left axis) and a histogram for response sizes (right axis, log scale). As the figure shows, *all* responses in this data set exceed the maximum size limits (1,232 and 1,500 bytes). The figure also more prominently shows the significant impact that the inclusion of additional signatures has on message size. Towards the left side of the plot (around 2,300 bytes) we see a small number of responses, the majority of responses fall in the 3,000 to 3,200 byte range. This can be explained by the number of NSEC3 records included, which each come with a corresponding signature. Table 2 shows how various response patterns lead to very predictable response sizes. Finally, Figure 3 also shows that the difference in response size for padded versus unpadded signatures becomes more prominent the more signatures are included in a message.

4.3 Putting the difference in perspective

So far we have seen that the differences in response size for real-world queries to the .nl zone between padded and unpadded Falcon-512 are small. Moreover, the difference in size does not lead to meaningful impact in terms of having a larger fraction of responses fall within size limits for unpadded Falcon-512. To put the size differences in perspective, we offset this size difference against the size differences that are a result of domain name length. The length of a domain name also impacts the size of a DNS response, as longer domain names obviously lead to larger responses. To put the impact in size difference between padded and unpadded signatures in perspective, we asked ourselves: *What is the distribution in domain name length in our real-world data and how does this compare to the size difference between padded and unpadded signatures?*

Figure 4 shows a histogram of the domain name length distribution for our data sets. As the figure shows, this distribution is long-tailed, with a median length of 14 bytes, with the vast majority of responses falling within +/- 8 bytes of the median. If we compare this to the signature size distribution show in Figure 1, we can see that the variance in domain name length is of the same order as the variance in unpadded signature size. In other words: the length of the domain name included in a query contributes similarly to message size as the size of a single Falcon-512 unpadded signature.

5 CONCLUSIONS

In this paper we set out to evaluate whether the use of unpadded Falcon signatures was beneficial to DNSSEC, in case it could make DNS messages smaller, respecting the MTU size limits (1,500 bytes or 1,280 bytes). We base our results on an empirical approach using real DNS query data from a large ccTLD to directly compare the impact of padded and unpadded Falcon signatures on DNSSEC message sizes in an operational scenario. From the analysis of the empirical message size distributions, we conclude the following:

Message size differences – For responses to existing domains (NOERROR): our results show that the difference in message size between padded and unpadded signatures is very small. In fact, we consider the difference insignificant and insufficient to make a big difference in terms of increasing the number of responses that fall within the size limits of a single packet (such as 1,500 or 1,232 bytes). The use of unpadded signatures does not lead to an appreciable increase in responses that fall within these limits.

For responses to non-existing domains (NXDOMAIN): Although the difference in message sizes between the two types of signatures (padded vs. unpadded) was greater for NXDOMAIN responses, these responses were already very large due to the presence of multiple NSEC3 records and their corresponding signatures. The use of unpadded signatures did not help to better fit these large messages within the MTU limits.

We show that, for the data considered in this paper, unpadded Falcon signatures for DNSSEC produce a negative result in terms of reducing DNS message sizes. The difference is too small to make a practical difference and does not reduce the need for multiple packets or TCP fallbacks.

Padded or unpadded for DNSSEC? – Given the lack of significant benefit in message size, standardization of a fixed-size, predictable format such as padded may be preferable, as it makes implementations of DNSSEC more predictable and less prone to implementation errors.

REFERENCES

[1] [n. d.]. 2020 — dnsflagday.net. https://www.dnsflagday.net/2020/. [Accessed 29-04-2025].

[2] [n. d.]. falcon.h — falcon-sign.info. https://falcon-sign.info/impl/falcon.h.html. [Accessed 11-04-2025].

[3] 2022. Falcon — falcon-sign.info. https://falcon-sign.info. [Accessed 25-03-2025].

[4] Gorjan Alagic. 2025. *Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process.* https://doi.org/10.6028/nist.ir.8545

[5] Jean-Philippe Aumasson, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hülsing, Panos Kampanakis, Stefan Kölbl, Tanja Lange, et al. 2019. SPHINCS+ — sphincs.org. https://sphincs.org. [Accessed 25-03-2025].

[6] Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stéhlé. [n. d.]. Dilithium — pq-crystals.org. https://pq-crystals.org/dilithium/. [Accessed 25-03-2025].

[7] Andrew Fregly, Roland van Rijswijk-Deij, Moritz Müller, Peter Thomassen, Caspar Schutijser, and Taejoong Chung. 2024. *Research Agenda for a Post-Quantum DNSSEC.* Internet-Draft draft-fregly-research-agenda-for-pqc-dnssec-02. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-fregly-research-agenda-for-pqc-dnssec/02/ Work in Progress.

[8] Jason Goertzen and Douglas Stebila. 2023. Post-Quantum Signatures in DNSSEC via Request-Based Fragmentation. In *Post-Quantum Cryptography: 14th International Workshop, PQCrypto 2023, College Park, MD, USA, August 16–18, 2023, Proceedings* (College Park, MD, USA). Springer-Verlag, Berlin, Heidelberg, 535–564.

[9] Shumon Huque, Christian Elmerot, and Ólafur Guðmundsson. 2025. *Compact Denial of Existence in DNSSEC.* Internet-Draft draft-ietf-dnsop-compact-denial-of-existence-07. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-ietf-dnsop-compact-denial-of-existence/07/ Work in Progress.

[10] Moritz Müller, Jins de Jong, Maran van Heesch, Benno Overeinder, and Roland van Rijswijk-Deij. 2020. Retrofitting post-quantum cryptography in internet protocols: a case study of DNSSEC. *SIGCOMM Comput. Commun. Rev.* 50, 4 (Oct. 2020), 49–57. https://doi.org/10.1145/3431832.3431838

[11] Moritz Müller, Willem Toorop, Taejoong Chung, Jelte Jansen, and Roland van Rijswijk-Deij. 2020. The Reality of Algorithm Agility: Studying the DNSSEC Algorithm Life-Cycle. In *Proceedings of the ACM Internet Measurement Conference* (Virtual Event, USA) *(IMC '20)*. Association for Computing Machinery, New York, NY, USA, 295–308. https://doi.org/10.1145/3419394.3423638

[12] Deepraj Soni, Kanad Basu, Mohammed Nabeel, Najwa Aaraj, Marcos Manzano, and Ramesh Karri. 2021. *FALCON.* Springer International Publishing, Cham, 31–41. https://doi.org/10.1007/978-3-030-57682-0_3

[13] Olivier van der Toorn, Moritz Müller, Sara Dickinson, Cristian Hesselman, Anna Sperotto, and Roland van Rijswijk-Deij. 2022. Addressing the challenges of modern DNS: a comprehensive tutorial. *Computer Science Review* 45 (2022), 100469. https://doi.org/10.1016/j.cosrev.2022.100469

[14] Roland van Rijswijk-Deij, Anna Sperotto, and Aiko Pras. 2014. DNSSEC and its potential for DDoS attacks: a comprehensive measurement study. In *Proceedings of the 2014 Conference on Internet Measurement Conference* (Vancouver, BC, Canada) *(IMC '14)*. Association for Computing Machinery, New York, NY, USA, 449–460. https://doi.org/10.1145/2663716.2663731