


# Using Compact DNSSEC and Self-Signed Certificate to Improve Security and Privacy for Second-Level Domain Resolution

Lanlan Pan<sup>1</sup> <sup>a</sup>, Ruonan Qiu<sup>2</sup> and Minghui Yang<sup>2</sup>

<sup>1</sup>University of Science and Technology of China, Anhui, China

<sup>2</sup>Guangdong OPPO Mobile Telecommunications Corp. Ltd., Guangdong, China

**Keywords:** DNS, Compact, DNSSEC, DoT, DoQ, DoDTLS, Self-Signed, DDoS, Dane, NS, TLSA, SLD.

**Abstract:** DNS is vulnerable to domain hijack attacks and user privacy leakage. DNSSEC is to defend against the domain hijack attack. However, full zone DNSSEC increases the risk of DDoS attacks. In this paper, we propose a secure resolution scheme with compact DNSSEC and self-signed certificates to improve security and privacy for SLD. The compact DNSSEC enhances the security of the NS of SLD. Based on the cooperation of DANE and compact DNSSEC, the authoritative server of SLD can use the self-signed certificates to provide a secure resolution service to mitigate user privacy leakage. Our scheme can reduce the operational burden of full zone DNSSEC and mitigate the DDoS risk for the authoritative server of SLD.

## 1 INTRODUCTION

Domain Name System (DNS) (Mockapetris, 1987) is a critical internet protocol that translates domain names into IP addresses. However, its plaintext traffic makes it vulnerable to domain hijack attacks and user privacy leakage (Schmid, 2021a). As Figure 1 shows, some proposals exist to improve the security and privacy of DNS protocol. DNS security extensions (DNSSEC) (Hoffman, 2023) has been primarily deployed on root servers and top-level domain (TLD) servers to defend against the domain hijack attack. DoT (Hu et al., 2016), DoQ (Huitema et al., 2022), DoDTLS (Reddy et al., 2017) and DoH (Hoffman and McManus, 2018) are deployed on some recursive resolvers to protect user privacy.

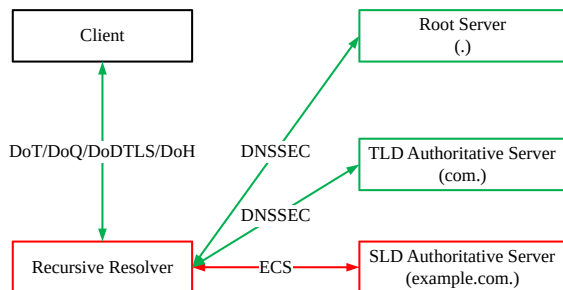



Figure 1: DNS Resolution.

<sup>a</sup>  <https://orcid.org/0000-0002-1771-2683>

### 1.1 Challenges

However, there are still some challenges to the second-level domains (SLD) resolution between recursive resolver and SLD authoritative server.

- ECS Privacy Leakage.** As Figure 1 shows, the EDNS client subnet (ECS) extension (Contavalli et al., 2016) aims to address the DNS response accuracy problem of public resolvers, however, the recursive resolver leaks the client subnet information on the resolution path to the authoritative server of SLD. Kintis (Kintis et al., 2016) pointed out that ECS makes DNS communications less private: the potential for mass surveillance is greater and stealthy, highly targeted DNS poisoning attacks become possible. Therefore, it is valuable to enhance privacy protection for the queries from the recursive resolver to the authoritative server of SLD.
- DNSSEC Low Deployment on SLD.** The main design of DNSSEC is cryptographic and technical complex (Hoffman, 2023) (Schlyter, 2004) (van Dijk, 2021), especially on the DNSSEC extensions such as NSEC (Schlyter, 2004) and NSEC3 (Laurie et al., ). Both NSEC and NSEC3 can provide the authenticated NXDOMAIN responses. NSEC3 is used to prevent the zone enumeration. Therefore, the operation burden of DNSSEC deployment is heavy (Elliott and Mox-

ley, 2023) (ISC, 2024). Internet corporation for assigned names and numbers (ICANN) presents the deployment statistics of DNSSEC in SLDs, which shows that there are only 4% SLDs in the 'com' zone deployed DNSSEC until October 2024 (ICANN, 2024).

3. **DDoS Risk.** DNS random subdomain attacks and amplification attacks are commonly used distributed denial-of-service (DDoS) attacks (Kaplan and Feibish, 2021) (Nawrocki et al., 2021). DNS random subdomain attack can overwhelm both the recursive resolver and the authoritative server, causing them to become unresponsive or even fail. As analyzed by Nexusguard, the DDoS amplification power of the authoritative server of SLD could be surged to more than 45X after deploying DNSSEC (Nexusguard, 2019).

## 1.2 Contribution

The contributions of this paper are as follows.

- We propose a secure resolution scheme with a compact DNSSEC and self-signed certificate to address the security and privacy challenges on SLD resolution between recursive resolver and SLD authoritative server.
- We provide a detailed explanation of the compact DNSSEC scheme. It is specifically targeting the NS/A/AAAA/TLSA resource record sets (RRsets) associated with NS resource record (RR) (Mockapetris, 1987), aimed to ease the operation burden of DNSSEC deployment and reduce the DDoS amplification power.
- We introduce the authoritative server of SLD to provide the secure resolution service with a self-signed certificate, and publish a domain-based authentication of named entities (DANE) TLSA record (Hoffman and Schlyter, 2012) for the self-signed certificate information.
- We introduce the recursive resolver to verify the RRSIG records provided by the compact DNSSEC and make secure resolution through the DoT/DoQ/DoDTLS channel to mitigate the ECS privacy leakage.
- We make the discussion and evaluation of our scheme to assess its effectiveness.

## 1.3 Paper Organization

The rest of this paper is outlined as follows. Section 2 presents the related work. Section 3 describes our scheme. Section 4 presents the discussion and evaluation. Finally, in section 5, we conclude the paper.

## 2 RELATED WORK

DNSSEC (Hoffman, 2023) adds cryptographic signatures to existing DNS records, and a recursive resolver can verify the signatures to ensure the response DNS records are not tampered with. Since DNSSEC covers the full zone of SLD by default, which results in a significant DDoS amplification factor. NSEC and NSEC3 (Schlyter, 2004) (Laurie et al., ) (van Dijk, 2021) (Miek, 2014) provide the authenticated NX-DOMAIN responses, which should keep updated with any subdomain change in the entire zone of SLD. By caching NSEC/NSEC3 responses, recursive resolvers can mitigate the random subdomain attacks. Moreover, NSEC3 requires additional cryptographic operations compared to NSEC. Therefore, it is valuable to design a compact DNSSEC scheme to reduce the operation burden and mitigate the DDoS risk.

Murakami et al. (Murakami et al., 2023) proposed a trustworthy domain name resolution method using PKI-based certificates with DoT-enabled authoritative DNS servers. They extend the DoT to the authoritative server of SLD and let the end terminal make the PKI-based certificate validation. The authoritative server of SLD is assumed to be trusted if the certificate is an OV/EV certificate. Otherwise, it is assumed to be untrusted if the certificate is DV. However, the OV/EV/DV certificate should be issued by a widely known certificate authority (CA), with additional operation burden and economic cost. Furthermore, the terminal sends the name resolution request to the authoritative server of SLD, which will increase the DDoS risk. Therefore, it is better to let the recursive resolver send the DoT queries to the authoritative server of SLD, which is compatible with exists terminal function and mitigates the DDoS risk.

Gillmor et al. (Gillmor et al., 2024) discussed the deployment of opportunistic encrypted transport in the recursive-to-authoritative hop of the DNS ecosystem. They suggested using the PKI-based certificate issued by a widely known CA or the TLS DNSSEC chain extension (Dukhovni et al., 2021) with the DANE TLSA support. The recursive resolver should verify the authoritative server's identity. The identity would presumably be based on the NS name used for a given query or the IP address of the authoritative server.

Sunahara et al. (Sunahara et al., 2022) proposed an architecture that encrypts all DNS communications with DoH. They extend the DoH protocol to the communication between the recursive resolvers and the authoritative servers. The encryption approach helps to protect user privacy all along the DNS communication path.

Table 1: The NS/A/AAAA/TLSA Records Associated With NS.

example.com.	345600	IN	NS	ns1.example.com.
example.com.	345600	IN	NS	ns2.example.com.
ns1.example.com.	345600	IN	A	11.22.33.44
ns1.example.com.	345600	IN	AAAA	::11.22.33.44
ns2.example.com.	345600	IN	A	55.66.77.88
ns2.example.com.	345600	IN	AAAA	::55.66.77.88
._853._tcp.ns1.example.com.	3600	IN	TLSA	( 3 1 1 63cbfcfa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364 )
._853._udp.ns1.example.com.	3600	IN	TLSA	( 3 1 1 63cbfcfa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364 )
._853._tcp.ns2.example.com.	3600	IN	TLSA	( 3 1 1 63cbfcfa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364 )
._853._udp.ns2.example.com.	3600	IN	TLSA	( 3 1 1 63cbfcfa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364 )

### 3 OUR SCHEME

As shown in Figure 2, in this section, we describe a scheme with compact DNSSEC and self-signed certificate to improve security and privacy for SLD.

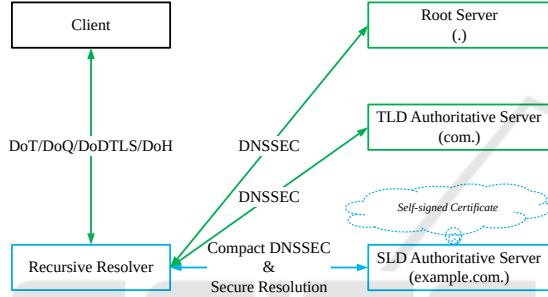


Figure 2: Our Scheme.

Take an example of SLD ‘example.com’. To simplify, we assume that the NS records are following the same TLD ‘com’ with the SLD ‘example.com’.

We mark the administrator of SLD as  $ADM_{slid}$ , the authoritative server of SLD as  $AS_{slid}$ , the recursive resolver as  $RS$ , the DNSSEC key signing key pair (KSK) of SLD as  $KSK_{slid}$ , the DNS zone signing key pair (ZSK) of SLD as  $ZSK_{slid}$ .

#### 3.1 Provide Secure Resolution Service with Self-Signed Certificate for SLD

$ADM_{slid}$  should generate a private key ( $d_{as}$ ) and issue a self-signed X.509 certificate ( $C_{as}$ ) for the corresponding public key ( $pub_{as}$ ).  $C_{as}$  is used for  $AS_{slid}$ ’s secure resolution service. To simplify, in this paper, we assume that all name servers of the SLD share the same self-signed certificate.

Assumed that  $ADM_{slid}$  has configured the NS records for the SLD: ‘ns1.example.com’ and ‘ns2.example.com’. The NS records should be written into the subjectAltName extension field of  $C_{as}$  (Cooper et al., 2008). The two  $AS_{slid}$  servers (‘ns1.example.com’ and ‘ns2.example.com’) can provide secure resolution services on port 853 with

$C_{as}$ . RFC9539 (Gillmor et al., 2024) discussed more operation details.

#### 3.2 Publish the TLSA Records

As Table 1 shows,  $ADM_{slid}$  should define the well-known subdomains (‘\_853.\_tcp’ and ‘\_853.\_udp’) for each NS record to publish its  $C_{as}$  information and configure the corresponding TLSA records (Hoffman and Schlyter, 2012). The TLSA record indicates the digest of the subject public key of  $C_{as}$ , marked as  $DgstSPK_{as}$ . The ‘\_853.\_tcp’ subdomain is for DoT service run on TCP port 853, and the ‘\_853.\_udp’ subdomain is for DoQ/DoDTLS service run on UDP port 853.

#### 3.3 Configure Compact DNSSEC

$ADM_{slid}$  should configure compact DNSSEC for ‘example.com’ to cover the critical records: the delegation signer (DS) record, the DNSKEY records, and the records associated with NS.

##### Publish the DS Record to TLD.

1.  $ADM_{slid}$  generates the DNSKEY RRsets for ‘example.com’, which contains the public  $KSK_{slid}$  and the public  $ZSK_{slid}$ .
2.  $ADM_{slid}$  calculates the hash of the public  $KSK_{slid}$  and marks it as  $DS_{slid}$ . generates the DS record of  $KSK_{slid}$ , which contains the hash of the public  $KSK_{slid}$ , and marked as  $DS_{slid}$ .
3.  $ADM_{slid}$  publishes  $DS_{slid}$  as the DS record of ‘example.com’ to the TLD ‘com’.
4. The TLD ‘com’ signs the RRSIG for  $DS_{slid}$  with its own private ZSK.

##### Sign the DNSKEY RRSIG of SLD.

1.  $ADM_{slid}$  signs the RRSIG for DNSKEY RRsets of example.com with the private  $KSK_{slid}$ .

##### Sign the RRSIGs associated with the NS of SLD.

1.  $ADM_{slid}$  signs the RRSIG for NS RRsets of example.com with the private  $ZSK_{slid}$ .

2.  $ADM_{slid}$  signs the RRSIG for A/AAAA RRsets of each NS record with the private  $ZSK_{slid}$ .
3.  $ADM_{slid}$  signs the RRSIG for the corresponding TLSA record of each NS with the private  $ZSK_{slid}$ .

### 3.4 Gain Trustworthy Records Associated with the NS of SLD

Based on the compact DNSSEC configuration and secure resolution service with a self-signed certificate,  $RS$  can gain trustworthy records associated with the NS of the SLD.

#### Verify the DS RRSIG and DNSKEY RRSIG.

$RS$  must verify the DS RRSIGs and DNSKEY RRSIGs following the DNSSEC chain.

To simplify, we assumed that the DNSSEC chain verification of the NS records follows the same TLD ‘com’ with the SLD in this paper. Note that the DNSSEC chain verification of the NS records can also support the scenarios that the different TLD (such as ‘net’, ‘org’) of NS records with the SLD.

1.  $RS$  makes DNSSEC resolution from root to TLD ‘com’, gets the DS record, DS RRSIG record, and NS records of ‘example.com’ from TLD.
2.  $RS$  makes DNSSEC resolution request to  $AS_{slid}$ , gets the DNSKEY RRsets and DNSKEY RRSIG of ‘example.com’.
3.  $RS$  verifies the DS RRSIG on the DS record with the public  $ZSK$  of TLD, checks the DS record matches the hash of KSK record, and ensures that  $KSK_{slid}$  is following the DNSSEC trust chain.
4.  $RS$  verifies the DNSKEY RRSIG on the DNSKEY RRsets with the public  $KSK_{slid}$ , and ensures that  $ZSK_{slid}$  is following the DNSSEC trust chain.

#### Verify the RRSIGs Associated with the NS of SLD.

Note that the records associated with NS require DNSSEC queries.

1.  $RS$  gets the NS RRsets and NS RRSIG from  $AS_{slid}$ , verifies the NS RRSIG with the public  $ZSK_{slid}$ , ensures that the NS RRsets are following the DNSSEC trust chain.
2.  $RS$  checks the A/AAAA RRsets of each NS record:
  - (a)  $RS$  gets the A RRsets and A RRSIG of the corresponding NS from  $AS_{slid}$ , verifies the A RRSIG with the public  $ZSK_{slid}$ , ensures that the A RRsets are following the DNSSEC trust chain.

- (b)  $RS$  gets the AAAA RRsets and AAAA RRSIG of the corresponding NS from  $AS_{slid}$ , verifies the AAAA RRSIG with the public  $ZSK_{slid}$ , ensures that the AAAA RRsets are following the DNSSEC trust chain.

3.  $RS$  gets the TLSA record and RRSIG of each NS from  $AS_{slid}$ , verifies the TLSA RRSIG with the public  $ZSK_{slid}$ , ensures that the TLSA record ( $DgstSPK_{as}$ ) is following the DNSSEC trust chain.
4.  $RS$  securely cache the trustworthy records of the SLD ‘example.com’, following DNS TTL configuration.

### 3.5 Make Secure SLD Resolution

Based on the trustworthy records and the secure resolution service with a self-signed certificate,  $RS$  can make secure SLD resolution with  $AS_{slid}$ .

1.  $RS$  receives other subdomain queries of example.com from the client.
2.  $RS$  makes a TLS connection with the secure resolution service of  $AS_{slid}$ , checks if the hash of the subject public key of the received  $C_{as}$  matches the TLSA record ( $DgstSPK_{as}$ ) of the NS, builds up the secure DoT/DoQ/DoDTLS channel.
3.  $RS$  makes DNS resolution through the secure channel, ensures that the DNS responses are trustworthy.
4.  $RS$  returns the trustworthy DNS responses to the client.

## 4 DISCUSSION AND EVALUATION

### 4.1 Compact DNSSEC Consideration

DNS is a hierarchical system with NS records as the core. There are many DNS hijack attacks around NS (Recursive, ) (Schmid, 2021b) (Ramdas and Muthukrishnan, 2019). DNSSEC can solve the hijack problem completely, while its entire zone RRSIGs increase the risk of high DDoS amplification attacks. The concerns about DDoS attack risk result in low DNSSEC deployment on SLD finally.

The compact DNSSEC focuses on protecting the critical records associated with NS. Table 2 compares the RRSIG amount with the Big O notation. Assumed that the SLD ‘example.com’ contains  $n$  subdomains.

Table 2: RRSIG Amount Comparison.

Scheme	Signed RRsets Scope	Amount of RRSIGs
Plaintext DNS	None	0
Full Zone DNSSEC	All records of all subdomains	$O(n)$
Compact DNSSEC	The NS/A/AAAA/TLSA records associated with NS	$O(1)$

Table 3: Certificate Scheme Comparison.

Scheme	Issuer	Configure TLSA Record and RRSIG	trust chain
Self-signed	$AS_{sld}$	Must	DNSSEC
PKI-based	widely known CA	Optional	widely known CA

With full zone DNSSEC, the amount of RRSIGs increases linearly ( $O(n)$ ) with the subdomains. Our compact DNSSEC has constant RRSIGs ( $O(1)$ ), limiting the DDoS amplification power by only signing the NS/A/AAAA/TLSA RRsets associated with NS.

## 4.2 Self-Signed Certificate Consideration

Table 3 shows the comparison of certificate schemes. The self-signed certificate is issued by  $AS_{sld}$ .  $RS$  must ensure that it is connected to the correct  $AS_{sld}$  with the correct certificate and fully follows the trust chain of DNSSEC. As described in section 3.4,  $ADM_{sld}$  must sign the RRSIG for the corresponding TLSA records of each NS of the SLD.

The PKI-based certificate is issued by A widely known CA.  $RS$  must ensure that it has connected to the correct  $AS_{sld}$  with the correct certificate following the trust chain of widely known CA. However,  $RS$  fully trusts all widely known CAs, which makes it vulnerable to certificate hijacking attacks. An attacker may hijack specific victim  $AS_{sld}$ , leading  $RS$  to make TLS connections with other malicious servers via the fake certificates, causing domain hijack.

PKI-based certificate can configure TLSA records and RRSIG to defend against the certificate hijacking attacks, requiring more operational and economic costs. Compared to the PKI-based certificate, the self-signed certificate is lightweight and following the pure DNSSEC trust chain to avoid the domain hijacking.

## 4.3 Secure SLD Resolution Consideration

When the ECS extension is enabled,  $RS$  leaks the client subnet information on the resolution path to  $AS_{sld}$ . Therefore, encrypting the DNS traffic between  $RS$  and  $AS_{sld}$  is valuable.  $RS$  can make a se-

cure resolution with  $AS_{sld}$  through the secure resolution service to deal with the ECS privacy leakage issue. Moreover, compact DNSSEC doesn't sign the records of the other subdomains not associated with NS, which can reduce the risk of DNS amplification attacks. The secure DoT/DoQ/DoDTLS resolution channel can also protect them from domain hijack attacks through trustworthy TLS authentication.  $RS$  can make a keep-alive TLS/DTLS connection for the hot SLDs to improve query speed and performance.

## 4.4 Scalability, Compatibility and Interoperability

Our scheme writes the NS records into the subjectAltName extension field of the self-signed certificate  $C_{as}$ , which can scale smoothly along with a massive number of SLDs served by the same authoritative servers. The TLSA configuration of SLDs is flexible with short-lived self-signed certificate since they only need to update to the same new TLSA record. Our scheme is compatible with existing DNS resolution architecture and DNSSEC infrastructure.  $RS$  makes a secure resolution with  $AS_{sld}$ , which does not interfere with the client, TLD, and root. Our scheme is interoperable with existing DNSSEC security solutions. The compact DNSSEC can reuse the existing operation tools of DNSSEC and make a shrinking deployment.

## 4.5 Scheme Comparison

Table 4 shows a comparison between our scheme and existing schemes. "√" means that the scheme has this property; "×" means that the scheme does not have this property.

Compared to the full zone DNSSEC with NSEC/NSEC3 (Schlyter, 2004) (Laurie et al., ), our compact DNSSEC scheme is focused on the records associated with NS, which can significantly reduce the operation burden of DNSSEC deployment. Moreover, our scheme does not provide authenticated NX-

Table 4: Scheme Comparison.

Scheme	DNSSEC	Authenticated NXDOMAIN Response	Prevent Zone Enumeration	Encrypted Resolution Path	Secure Resolution Service	DNS Amplification DDoS Attack
Plaintext DNS (Mockapetris, 1987)	×	×	×	×	×	×
DNSSEC with NSEC (Schlyter, 2004)	Full Zone	✓	Weak	×	×	✓
DNSSEC with NSEC3 (Laurie et al., )	Full Zone	✓	✓	×	×	✓
Murakami T., et al (Murakami et al., 2023)	×	×	×	$Client \rightleftharpoons AS_{sld}$	DoT	×
Gillmor D., et al (Gillmor et al., 2024)	×	×	×	$RS \rightleftharpoons AS_{sld}$	DoT/DoQ	×
Sunahara S., et al (Sunahara et al., 2022)	×	×	×	$Client \rightleftharpoons RS \rightleftharpoons AS_{sld}$	DoH	×
Our Scheme	Compact	×	×	$RS \rightleftharpoons AS_{sld}$	DoT/DoQ/DoDTLS	×

DOMAIN response, which can avoid all NXDOMAIN interval and signature calculations between subdomains. NSEC is weak to zone enumeration, and NSEC3 supports to prevent zone enumeration. Our scheme has no impact on zone enumeration. Therefore, the deployment of our scheme is much simpler than the full zone DNSSEC with NSEC/NSEC3.

Our scheme makes encrypted resolution between  $RS$  and  $AS_{sld}$ , which can defend against the passive monitoring of the client subnet information and mitigate the ECS privacy leakage problem. Compared with Murakami et al. (Murakami et al., 2023), our scheme does not influence the client and is compatible with existing resolution architecture. Compared with the full DoH service proposed by Sunahara et al. (Sunahara et al., 2022), our scheme chooses the lightweight DoT/DoQ/DoDTLS services.

Gillmor et al. (Gillmor et al., 2024) recommend transiting the DNS records to authenticate in the TLS handshake using the DNSSEC chain extension (Dukhovni et al., 2021). However, the DNSSEC chain extension requires  $AS_{sld}$  to construct the serialized authentication chain, and  $RS$  should verify the whole chain when setting up the TLS connection. Compared with (Gillmor et al., 2024), our scheme arranges the DNSSEC chain verification in an individual section 3.4.  $RS$  only needs to check if the hash of the received  $C_{as}$  matches the TLSA record of the NS in the TLS handshake process, which could be added to the CertificateVerify function on the  $RS$  side easily (Rescorla, 2018).

DNSSEC increases the DDoS amplification attack risk since the RRSIGs cover the entire zone subdomains. Compared with the full zone DNSSEC, our compact DNSSEC scheme only calculate RRSIG on the records associated with NS, which can limit the amplification power of the authoritative server of SLD.

## 4.6 Evaluation

We make the evaluation on a 64-bit Arch Linux computer with an AMD Ryzen 9 5900 12-core processor, 64GiB RAM. As mentioned in section 3, we choose the NIST elliptic curve P-256 (SP, 2023) to generate

the  $KSK$  and  $ZSK$ , and SHA256 is the hash function for RRSIG calculations (Pub, 2012). Our experiment code can be found in (Pan, 2024).

We make an evaluation on the four schemes with TCP connection: plaintext DNS, DNSSEC with NSEC, DNSSEC with NSEC3, and our scheme (DoT). To simplify, we configure only one A record for each subdomain in the evaluation. We query A records for the existing subdomains of the SLD and random non-existent subdomains, and calculate the average resolution time and payload size. We don't enable the aggressive NSEC (van Dijk, 2021) on the recursive resolver in the full zone DNSSEC evaluation.  $N$  represents the number of existing subdomains of the SLD.  $M$  represents the number of random non-existent subdomains.

### 4.6.1 Zone File Size

Table 5 shows the comparison of the zone file size of four schemes. As analyzed in section 4.1, plaintext DNS contains the minimum zone file size of the four schemes, and our compact DNSSEC scheme is approximate with plaintext DNS with constant RRSIGs ( $O(1)$ ). The zone file size of DNSSEC with NSEC/NSEC3 is about 16 times bigger than plaintext DNS and our scheme. The full zone DNSSEC will increase the RRSIG/NSEC/NSEC3 records linearly ( $O(n)$ ) when the number of subdomains increases, finally resulting in a large zone file size.

Table 5: Zone File Size (Bytes).

Schemes	Number of Existing Subdomains ( $N$ )			
	100	1000	10000	50000
Plaintext DNS	4085	33554	330143	1648649
DNSSEC with NSEC	52275	494113	4912291	24549305
DNSSEC with NSEC3	79185	596264	5734853	28573360
Our Scheme (DoT)	5273	34741	331331	1649811

### 4.6.2 Average Resolution Time

Table 6 compares the average resolution time on the existing subdomains of four schemes. As described in section 4.3, our scheme makes a single keep-alive DoT connection for all subdomains but does not cre-

ate a unique DoT connection for each subdomain. Therefore, our scheme gains the minimum resolution time of the four schemes in the evaluation when  $N \geq 1000$ . Note that, since TLS requires more time than pure TCP to setup the connection, our scheme consumes more resolution time when  $N = 100$ .

Table 6: Average Resolution Time (Milliseconds): Existing Subdomains.

Schemes	Number of Existing Subdomains ( $N$ )			
	100	1000	10000	50000
Plaintext DNS	0.027	0.023	0.023	0.028
DNSSEC with NSEC	0.025	0.024	0.024	0.026
DNSSEC with NSEC3	0.026	0.023	0.023	0.027
Our Scheme (DoT)	0.032	0.013	0.010	0.010

Table 7: Average Resolution Time (Milliseconds): Random Non-existent Subdomains ( $M = 50000$ ).

Schemes	Number of Existing Subdomains ( $N$ )			
	100	1000	10000	50000
Plaintext DNS	0.026	0.028	0.028	0.027
DNSSEC with NSEC	0.023	0.024	0.024	0.024
DNSSEC with NSEC3	0.024	0.023	0.023	0.023
Our Scheme (DoT)	0.009	0.009	0.010	0.010

Table 7 shows the comparison of the average resolution time on the random non-existent subdomains ( $M = 50000$ ) of four schemes. Similar to the existing subdomains, our scheme consumes the minimum resolution time of the four schemes since it makes a single keep-alive DoT connection, about 0.10 milliseconds.

#### 4.6.3 Average Payload Size

$L_{req}$  represents the average request payload size.  $L_{res}$  represents the average response payload size. The DDoS amplification factor is  $\frac{L_{res}}{L_{req}}$ .

Table 8: Average Request Payload Size (Bytes): Existing Subdomains.

Schemes	Number of Existing Subdomains ( $N$ )			
	100	1000	10000	50000
Plaintext DNS	51.16	50.99	50.96	50.96
DNSSEC with NSEC	62.16	61.99	61.96	61.96
DNSSEC with NSEC3	62.16	61.99	61.96	61.96
Our Scheme (DoT)	76.95	73.36	73.00	72.97

Table 8 and Table 9 compare the average request and response payload size on the existing subdomains of four schemes. The DDoS amplification factor of plaintext DNS is about 1.31; DNSSEC with NSEC/NSEC3 is about 3; our scheme is about 1.21.

Table 9: Average Response Payload Size (Bytes): Existing Subdomains.

Schemes	Number of Existing Subdomains ( $N$ )			
	100	1000	10000	50000
Plaintext DNS	67.16	66.99	66.96	66.96
DNSSEC with NSEC	185.16	184.99	184.96	184.96
DNSSEC with NSEC3	185.16	184.99	184.96	184.96
Our Scheme (DoT)	103.01	88.57	87.12	86.99

Table 10: Average Payload Size (Bytes): Random Non-existent Subdomains ( $M = 50000$ ).

Schemes	Request Payload Size	Response Payload Size
Plaintext DNS	54.96	99.96
DNSSEC with NSEC	65.96	556.46
DNSSEC with NSEC3	65.96	798.29
Our Scheme (DoT)	76.97	119.99

Our scheme has the minimum DDoS amplification factor of the four schemes since it makes a single keep-alive DoT connection.

Table 10 shows the comparison of the average request and response payload size on the random non-existent subdomains ( $M = 50000$ ) of four schemes. The DDoS amplification factor of plaintext DNS is about 1.82; DNSSEC with NSEC is about 8.44; DNSSEC with NSEC3 is about 12.10; our scheme is about 1.56. The DDoS amplification factor of our scheme is approximate with plaintext DNS, lower than 2. DNSSEC with NSEC/NSEC3 have high amplification factors since they include RRSIG and NSEC/NSEC3 records in the response payloads.

## 4.7 Limitation

In this paper, we don't create a new DNS extension but focus on enhancing the trustworthiness validation of the NS and privacy protection.  $AS_{sld}$  should enable compact DNSSEC and provide its secure resolution service on port 853.  $RS$  should make DNSSEC chain validation go down to the TLSA RRSIG and check if the hash of the subject public key of  $C_{as}$  matches the TLSA record. We setup the secure channel based on the standardized DoT/DoQ/DoDTLS, and don't discuss about other alternative solution such as DNSCurve (Bernstein, 2009). Our compact DNSSEC scheme does not cover the entire zone and does not deploy NSEC/NSEC3 to mitigate DNS random subdomain attacks. Alternatively, we recommend  $AS_{sld}$  and  $RS$  deploy subdomain whitelist scheme to mitigate DNS random subdomain attacks (Pan et al., 2024).

## 5 CONCLUSION

This paper describes a secure resolution scheme for SLD. Our scheme requires the domain administrator of SLD to generate a self-signed certificate to run the secure resolution service and make a compact DNSSEC configuration. The compact DNSSEC is shrinking from full zone DNSSEC, which can ease the operation burden of DNSSEC deployment. We focus on making the recursive resolver gain the trustworthy authoritative server addresses of SLD, set up a secure resolution channel by TLS, and finally defend against domain hijack and privacy leakage. The evaluation result shows that our scheme has a low DDoS amplification power, which can mitigate the DDoS amplification attack caused by full zone DNSSEC, especially when many bots send vast amounts of queries on critical SLD. Our future work is to do more impact evaluation on our scheme and deploy it on the DNS system.

## REFERENCES

- Bernstein, D. J. (2009). Dnscurve: Usable security for dns. <https://dnscurve.org/>.
- Contavalli, C., van der Gaast, W., Lawrence, D., and Kumari, W. (2016). Rfc 7871: Client subnet in dns queries.
- Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and Polk, W. (2008). Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile. Technical report.
- Dukhovni, V., Huque, S., Toorop, W., Wouters, P., and Shore, M. (2021). Rfc 9102 tls dnssec chain extension.
- Elliott, A. and Moxley, J. (2023). The sad story of dnssec.
- Gillmor, D., Salazar, J., and Hoffman, P. (2024). Rfc 9539: Unilateral opportunistic deployment of encrypted recursive-to-authoritative dns.
- Hoffman, P. (2023). Rfc 9364: Dns security extensions (dnssec).
- Hoffman, P. and McManus, P. (2018). Rfc 8484: Dns queries over https (doh).
- Hoffman, P. and Schlyter, J. (2012). The dns-based authentication of named entities (dane) transport layer security (tls) protocol: Tlsa. Technical report.
- Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and Hoffman, P. (2016). Rfc 7858: Specification for dns over transport layer security (tls).
- Huitema, C., Dickinson, S., and Mankin, A. (2022). Rfc 9250: Dns over dedicated quic connections.
- ICANN (2024). M11: Dnssec deployment in tld and sld. <https://usgv6-deploymon.antd.nist.gov/snap-all.html>.
- ISC (2024). Cve-2023-50868: Preparing an nsec3 closest encoder proof can exhaust cpu resources. <https://kb.isc.org/v1/docs/cve-2023-50868>.
- Kaplan, A. and Feibish, S. L. (2021). Dns water torture detection in the data plane. In *Proceedings of the SIGCOMM'21 Poster and Demo Sessions*, pages 24–26.
- Kintis, P., Nadji, Y., Dagon, D., Farrell, M., and Antonakakis, M. (2016). Understanding the privacy implications of ecs. In *Detection of Intrusions and Malware, and Vulnerability Assessment: 13th International Conference, DIMVA 2016, San Sebastián, Spain, July 7-8, 2016, Proceedings 13*, pages 343–353. Springer.
- Laurie, B., Sisson, G., Arends, R., and Blacka, D. Rfc 5155-dns security (dnssec) hashed authenticated denial of existence (2008). URL <https://tools.ietf.org/html/rfc5155>.
- Miek, G. (2014). Rfc 7129: Authenticated denial of existence in the dns.
- Mockapetris, P. (1987). Domain names-concepts and facilities. Technical report.
- Murakami, T., Shimabukuro, K., Sato, N., Nakagawa, R., Jin, Y., and Yamai, N. (2023). Trustworthy name resolution using tls certificates with dot-enabled authoritative dns servers. In *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 1121–1126. IEEE.
- Nawrocki, M., Jonker, M., Schmidt, T. C., and Wählisch, M. (2021). The far side of dns amplification: tracing the ddos attack ecosystem from the internet core. In *Proceedings of the 21st ACM Internet Measurement Conference*, pages 419–434.
- Nexusguard (2019). Dnssec fuels new wave of dns amplification. <https://www.nexusguard.com/blog/dnssec-fuels-new-wave-of-dns-amplification>.
- Pan, L. (2024). Compact dnssec for sld. [https://github.com/abbypan/compact\\_dnssec\\_dot\\_sld](https://github.com/abbypan/compact_dnssec_dot_sld).
- Pan, L., Qiu, R., and Yang, M. (2024). Asdwl: Mitigating dns random subdomain attacks for second level domain. In *2024 International Conference on Smart Applications, Communications and Networking (Smart-Nets)*, pages 1–4. IEEE.
- Pub, F. (2012). Secure hash standard (shs). *Fips pub*, 180(4).
- Ramdas, A. and Muthukrishnan, R. (2019). A survey on dns security issues and mitigation techniques. In *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, pages 781–784.
- Recursive, D. Nxnsattack: Recursive dns inefficiencies and vulnerabilities.
- Reddy, T., Wing, D., and Patil, P. (2017). Rfc 8094: Dns over datagram transport layer security (dtls).
- Rescorla, E. (2018). The transport layer security (tls) protocol version 1.3. Technical report.
- Schlyter, J. (2004). Rfc 3845: Dns security (dnssec) nextsecure (nsec) rdata format.
- Schmid, G. (2021a). Thirty years of dns insecurity: Current issues and perspectives. *IEEE Communications Surveys & Tutorials*, 23(4):2429–2459.



- Schmid, G. (2021b). Thirty years of dns insecurity: Current issues and perspectives. *IEEE Communications Surveys & Tutorials*, 23(4):2429–2459.
- SP, N. (2023). Recommendations for discrete logarithm-based cryptography.
- Sunahara, S., Jin, Y., and Iida, K. (2022). A proposal of doh-based domain name resolution architecture including authoritative dns servers. In *2022 32nd International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–3. IEEE.
- van Dijk, P. (2021). Rfc 9077: Nsec and nsec3: Ttls and aggressive use.

