Can NSEC5 be practical for DNSSEC deployments?*

Dimitrios Papadopoulos†
Hong Kong University of Science and Technology & University of Maryland
dipapado@cse.ust.hk

Duane Wessels
Verisign Labs
dwessels@verisign.com

Shumon Huque*
Salesforce
shuque@gmail.com

Moni Naor
Weizmann Institute
moni.naor@weizmann.ac.il

Jan Včelák‡
NS1
jvcelak@ns1.com

Leonid Reyzin
Boston University
reyzin@cs.bu.edu

Sharon Goldberg
Boston University
goldbe@cs.bu.edu

ABSTRACT

NSEC5 is a new proposal for providing *authenticated denial of existence* for DNSSEC, *i.e.,* for securely responding to DNS queries for names that do not exist in a zone. NSEC5 simultaneously guarantees two security properties: (1) privacy against zone enumeration, and (2) integrity of zone contents, even if an adversary compromises the authoritative nameserver responsible for responding to DNS queries for the zone. By contrast, today's DNSSEC protocol can guarantee one of these properties, but not both. This paper argues that NSEC5 not only improves DNS security, but is also practical and performant. To that end, we present a new version of NSEC5 that uses elliptic curve cryptography to achieve small DNSSEC responses and fast query-processing times. We also extend widely-used DNS software to present the first implementations of NSEC5 for an authoritative nameserver and a recursive resolver. We believe that our performance results indicate that NSEC5 can be a practical solution for DNSSEC deployments.

1. INTRODUCTION

NSEC5 is a new proposal for providing *authenticated denial of existence* for DNSSEC, *i.e.,* for responding to DNS queries ("What is the IP address of `aWa2j3.com`?") for names that do not exist in a zone ("NXDOMAIN: `aWa2j3.com` does not exist in the `.com` zone.") NSEC5 has two key security properties.

First, NSEC5 provides *strong integrity*, protecting the integrity of the zone contents even if an adversary compromises the authoritative nameserver responsible for responding to DNS queries for the zone. Hardening the DNS against external compromise seems to be an increasingly important security goal [62], especially in light of recent attacks [9, 10, 12, 32, 44].

Second, NSEC5 provides *privacy* against offline *zone enumeration* [7, 18, 22, 52, 58, 61, 75, 76, 78], where an adversary makes a small number of online DNS queries and then processes them offline in order to learn all the domain names in a zone. Zone enumeration can be used to identify routers, servers or other 'things' (thermostats, fridges, baby monitors, *etc.*) that could then be targeted in more complex attacks. An enumerated zone can also be "a source of probable e-mail addresses for spam, or as a key for multiple WHOIS queries to reveal registrant data that many registries may have legal obligations to protect" [52] (*e.g.,* per EU data protection laws [66], [13, pg. 37]). Several publicly available network reconnaissance tools can be used to launch zone-enumeration attacks [2, 7, 22, 58, 61, 75].

While today's DNSSEC protocol has several mechanisms for authenticated denial of existence, they all either fail to provide integrity against a compromised nameserver (*i.e.,* online signing used in NSEC3 White Lies [36] and Minimally-Covering NSEC [77]), or fail to prevent zone enumeration (NSEC [14], NSEC3 [52]). In fact, zone enumeration is an issue introduced by DNSSEC, and is not a possible attack on legacy DNS.

Optimizing and implementing NSEC5. The first cryptographic construction for NSEC5 was presented in [40], but it was never implemented, tested or fully specified. Moreover, the construction in [40] was based on the RSA cryptosystem. RSA is widely used in today's DNSSEC deployments [69, 74], but there is currently serious discussion about replacing RSA with elliptic curve cryptography (ECC) for improved performance and security [43, 68, 72]. Thus, the community is unlikely to adopt a new mechanism based on RSA.

This paper presents a new cryptographic construc-

*Full version from February 13, 2017.
†Substantial parts of this work conducted at Verisign Labs.
‡Substantial parts of this work conducted at CZ.NIC.

tion for NSEC5 that uses elliptic curve cryptography (ECC) (Section 3.5),[1] and presents formal cryptographic proofs of its security (Appendix B). We further optimize NSEC5 with several DNS-level protocol optimizations (Section 4). We fully specify NSEC5,[2] and present a full implementation of an authoritative nameserver and recursive resolver that support both RSA- and ECC-based NSEC5 (Section 6). (For the nameserver implementation, we extend the Knot DNS 1.6 [3]. For the recursive resolver, we extend Unbound 1.5.9.)

Performance. We show that our ECC-based NSEC5 can be viable even for high-throughput scenarios. Throughput at our authoritative nameserver easily scales to a few tens of thousands of queries per second (64K query/second) on a moderately-sized multi-core server (*i.e.,* 24 threads on 40 virtual cores). This is an order of magnitude larger than the average negative response rate at single server in the DNS's root zone [1]. In fact, our ECC-based NSEC5 nameserver implementation achieves a throughput that is about 2x higher than the only widely-deployed nameserver implementation that prevents zone enumeration and is compliant with the DNSSEC standards (*i.e.,* PowerDNS's implementation of online signing via NSEC3 White Lies [8]). Meanwhile, the performance of our NSEC5-ready recursive resolver (Section 7.3) is comparable to DNSSEC's existing denial-of-existence mechanisms.

Response lengths. Response length is another key parameter to consider when evaluating NSEC5.

DNSSEC naturally amplifies the length of DNS response by including cryptographic keys and digital signatures. Several unfortunate things occur when long DNSSEC responses no longer fit in a single IP packet [60, 61, 63]. First, responses sent over UDP can be fragmented across multiple IP fragments, and thus risk being dropped by a middlebox that blocks IP fragments [67, 71] or being subject to an IP fragmentation attack [41]. Alternatively, the resolver can resend the query over TCP [30, 56], harming performance (due to roundtrips needed to establish a TCP connection) and availability (because some middleboxes block DNS over TCP) [67]. Worse yet, long DNSSEC responses can be used to amplify DDoS attacks [35]. In a DDoS amplification attack, a botnet sends nameservers many small DNS queries that are spoofed to look like they come from a victim machine, and the nameservers respond by pelting the victim machine with many long DNSSEC responses. Long DNSSEC responses increase the volume of traffic that arrives at the victim.

Fortunately, recent measurements [71, Fig. 10] found that DNSSEC's existing authenticated denial of existence records (NSEC and NSEC3 records) are not the worst offenders in terms of DNSSEC length amplification. We show (Section 7.1) that our ECC-based NSEC5 responses easily fit into a single IP packet, and have lengths that are comparable to ECC versions of the current DNSSEC protocol (*i.e.,* NSEC3 with ECDSA signatures). In fact, ECC-based NSEC5 produces NXDOMAIN responses that are *shorter* than those produced by today's dominant DNSSEC deployment configuration, which has a lower security level (*i.e.,* NSEC3 with 1024-bit RSA signatures [69, 74])!

Transition. We conclude (Section 10) by discussing mechanisms for transitioning NSEC5 into the DNSSEC protocol. Given that the adoption of new cryptographic algorithms may be on the horizon (*e.g.,* digital signatures over Edwards elliptic curves [68,79]), now may also be a good time to consider the transition to NSEC5.

2. TRADEOFFS IN TODAY'S DNSSEC

We start by reviewing the issues that lead to the development of NSEC5 for DNSSEC. (See *e.g.,* [78] for a historical overview of the full DNSSEC protocol.)

With DNSSEC, a trustworthy *zone owner* is trusted to determine the set of names (`www.example.com`) present in the zone and their mapping to corresponding values (172.18.216.34). *Nameservers* receive information from the zone owner, and respond to DNS queries for the zone made by *resolvers*. DNSSEC's schemes for authenticated denial of existence reflect tradeoffs between integrity and privacy against zone enumeration. We describe each scheme and its tradeoffs below:

NSEC (RFC 4034 [14]). The NSEC record is defined as follows. The trusted owner of the zone prepares a lexicographic ordering of the names present in a zone, and uses the private *zone signing key (ZSK)* to sign a record containing each consecutive pair of names. The precomputed NSEC records are then provided to the nameserver. Then, to prove the non-existence of a name (`x.example.com`), the nameserver returns the NSEC record corresponding to the pair of existent names that are lexicographically before and after the non-existent name (`w.example.com` and `z.example.com`), with its associated DNSSEC signatures.

NSEC provides **strong integrity**—it not only protects against network attackers that intercept and attempt to alter DNSSEC responses, but is also robust to a malicious nameserver. This is because NSEC records are precomputed and signed by the trusted owner of the zone, and so the nameserver does not need to know the private ZSK in order to produce a valid NSEC record. Without the private ZSK, a malicious nameserver cannot sign bogus DNSSEC responses.

On the other hand, NSEC is highly vulnerable to zone enumeration attacks, where an adversary makes a number of *online* queries to the nameserver to collect all the NSEC records, and thus trivially learns all the names

[1]We first described this cryptographic construction in a short technical report [39].

[2]The full specification is in our IETF internet draft [73].

in the zone. Several network reconnaissance tools use NSEC records to enumerate DNS zones [2, 5, 58, 61].

NSEC3 (RFC 5155 [52]). NSEC3 is meant to raise the bar for zone enumeration attacks. The trusted owner of the zone cryptographically hashes all the names present in the zone using SHA1, lexicographically orders all the hash values, and uses the private ZSK to sign a NSEC3 record containing every consecutive pair of hashes. To prove the non-existence of a name, the nameserver returns the precomputed NSEC3 record (and the associated DNSSEC signatures) for the pair of hashes lexicographically before and after the *hash* of the non-existent name.

When NSEC3 records are precomputed, it also provides strong integrity. However, [22, 76] demonstrated (and RFC 5155 [52, Sec. 12.1.1] acknowledged) that hashing does not eliminate zone enumeration. To enumerate a zone that uses NSEC3, the adversary again makes a number of *online* queries to the nameserver to collect all the NSEC3 records, and then uses an *offline* dictionary attack to crack the hash values in the NSEC3 records, thus learning the names present in the zone. These offline attacks will only become faster as new tools come online [5, 7, 75] and technologies for fast hashing continue to improve (*e.g.,* GPUs [76], ASICs).

Online signing with NSEC3 White Lies (RFC 7129 [36]). Neither NSEC nor NSEC3 prevent zone enumeration. As a result, the DNS community introduced a radically different approach that prevented zone enumeration at the cost of sacrificing strong integrity. DNSSEC *online signing* requires the nameserver to hold the secret zone-signing key (ZSK), and to use it to generate NSEC3 responses on the fly. Crucially, online signing does not provide strong integrity—it protects only against network attackers that intercept DNSSEC responses, but integrity is totally lost if the nameserver is compromised, because the nameserver holds the secret ZSK that can be used to sign bogus DNSSEC responses. We call this **weak integrity**.

RFC 7129 [36] describes an online signing approach called "NSEC3 White Lies" which is supported by at least one major nameserver implementation (PowerDNS). NSEC3 White Lies requires the nameserver to use the secret ZSK to generate, on the fly, an NSEC3 record that covers a query with the minimal pair of hash values.[3] That is, given a query α and its hash value $h(\alpha)$, the nameserver generates an NSEC3 record containing the pair of hashes $(h(\alpha)-1, h(\alpha)+1)$, and signs the NSEC3 record with the private ZSK. Because the NSEC3 record only contains information about the queried name α, but not about any name present in the zone, it provides **privacy against zone enumeration**. Offline zone enumeration attacks no longer work. Instead, an adversary can only enumerate the zone by brute force, sending an online query to the nameserver for each name that it suspects is in the zone.

	no online crypto	weak integrity	strong integrity	privacy
legacy DNS	✓	*X*	*X*	✓
(plain) NSEC or (plain) NSEC3	✓	✓	✓	*X*
online signing, e.g. White Lies	*X*	✓	*X*	✓
NSEC5	*X*	✓	✓	✓

Table 1: Properties of NSEC*. Note that [40] proved that it is impossible to provide both privacy and weak integrity without online crypto.

NSEC3 White Lies also has a helpful backwards-compatiblity property for resolvers: resolvers just need to validate the NSEC3 record, but do not need to know or care whether the server is doing online signing (with NSEC3 White Lies) or not (with plain NSEC3).

3. NSEC5 & ITS SECURITY PROPERTIES

NSEC5 was introduced in [40, 57], to provide both privacy against zone enumeration and strong integrity. NSEC5 is very similar to NSEC3, except that we replace the cryptographic hashes used in NSEC3 with the hashes computed by a *verifiable random function (VRF)* [54]. Table 1 summarizes properties of NSEC5.

We first revisit the exposition in [57] to show how NSEC5 can be generically constructed from a VRF. We then review the RSA-based NSEC5 construction from [40] by showing how to construct a VRF from RSA. RSA-based NSEC5 is simpler to understand and implement. However, recent years have seen the DNS community aiming to replace RSA with elliptic curve cryptography (EC) [43, 68, 72]. The goal of this replacement is to shorten the length of DNSSEC responses while achieving a higher security level. (ECDSA signatures over 256-bit elliptic curves are 256 bits long and are understood to have an $\ell = 128$-bit security level, comparable to 3072-bit RSA; today, most zones use 1024-bit RSA [69, 74].) As such, the present paper introduces a new version of NSEC5, based on elliptic curves. To do this, we construct a VRF from elliptic curves using a construction implicit in several earlier papers [33, 38]. However, because these papers do not prove that the construction is a VRF, we provide new cryptographic proofs of its security in Appendix B.

3.1 Verifiable Random Functions (VRF).

A VRF [54] is essentially the public-key version of a keyed cryptographic hash. A VRF comes with a public-key pair (PK, SK). Only the holder of the private key SK can compute the hash, but anyone with public key

[3] RFC4470 [77] also proposes "Minimally Covering NSEC Records" an analogous online signing approach that uses NSEC records instead of NSEC3 records. We omit further discussion of this approach because it is not supported by major nameserver implementations (*i.e.,* BIND, PowerDNS, Microsoft DNS, Knot DNS, *etc.*).

PK can verify the hash. A VRF hashes an input α using the private key SK

$$\beta = F_{SK}(\alpha)\,.$$

The **collision-resistance** guarantee of a VRF is similar to that of a cryptographic hash function. The **pseudo-randomness** of a VRF guarantees that β is indistinguishable from random by anyone who does not know the private key SK. The private key SK is also used to construct a *proof* π that β is the correct hash output

$$\pi = \Pi_{SK}(\alpha)\,.$$

The proof π is constructed in such a way that anyone holding the public key can validate that indeed $\beta = F_{SK}(\alpha)$. Finally, the VRF has a **trusted uniqueness** property that roughly requires that, given the VRF public key PK, each VRF input α corresponds to a unique VRF hash output β. More precisely, trusted uniqueness guarantees that, given a validly-generated PK, even an adversary that knows SK cannot produce a valid proof for a fake VRF hash output $\beta' \neq \beta$. (The word "trusted" here is used to indicate that we trust the key generation process, and are not concerned with uniqueness for untrusted keys.) See Appendix B for formal definitions.

All the VRFs we consider in this paper allow β to be computed directly from π by a simple operation, *i.e.,* hashing. This reduces communication, since communicating π alone (without β) suffices.

3.2 NSEC5 from VRFs.

NSEC5 uses a VRF to provide authenticated denial of existence for DNSSEC [57, Sec. 7]. We review the NSEC5 construction and three new types of DNSSEC records it requires: NSEC5, NSEC5KEY and NSEC5PROOF.

The NSEC5KEY. NSEC5 uses a VRF with its own keys. These keys are distinct from the ZSK that computes DNSSEC signatures. The private VRF key is known to both the nameserver and the trusted owner of the zone. Meanwhile, the private ZSK is only known to the trusted owner of the zone. Finally, resolvers get the public ZSK (in a DNSKEY record), and the public VRF key (in an NSEC5KEY record) using the standard mechanisms used to distribute keys in DNSSEC.

Why do we need two separate keys, namely the ZSK (for signing DNS records) and the VRF key (for NSEC5)? This allows us to separate our two security goals (*i.e.,* strong integrity and privacy against zone enumeration). To achieve strong integrity, we follow the approach in NSEC and NSEC3, and provide the private ZSK to the the trusted zone owner but not to the untrusted nameserver. On the other hand, any reasonable definition of privacy against zone enumeration must trust the nameserver; after all, the nameserver holds all the DNS records for the zone, and thus can trivially enumerate the zone. For this reason, we will provide the secret VRF key to the nameserver, and use the VRF *only* to deal with zone enumeration attacks.

In [40], cryptographic lower bounds were used to prove the nameserver must *necessarily* have some secret cryptographic key. However, we shall soon see that NSEC5 still provides strong integrity even if the nameserver's private key is compromised or made public—all that is lost is privacy against zone enumeration. This is contrast to any online signing approach, such as NSEC3 White Lies, where compromising the nameserver's secret key eliminates both integrity and privacy against zone enumeration (Table 2).

Precomputing NSEC5 records. The trusted owner of the zone uses the private VRF key SK to compute the VRF hashes of all the names present in the zone, lexicographically orders all the the hash values, and uses the private ZSK to sign a record containing every consecutive pair of hashes; each pair of hashes is an NSEC5 record. The precomputed NSEC5 records and their associated DNSSEC signatures are provided to the nameserver along with the private VRF key SK.

Responding with NSEC5 and NSEC5PROOFs. To prove the non-existence of a queried name α, the nameserver uses the private VRF key SK to obtain the VRF hash output $\beta = F_{SK}(\alpha)$ and the proof value $\pi = \Pi_{SK}(\alpha)$. The nameserver responds to the query with

1. an NSEC5PROOF record containing π, and[4]
2. the precomputed NSEC5 record (and the associated DNSSEC signatures) for the pair of hashes lexicographically before and after β.

NSEC5 is almost identical to NSEC3, except that NSEC3 does not have a 'PROOF' record because resolvers can hash α by themselves. (Indeed, the public nature of NSEC3's hash function is exactly the cause of its vulnerability to offline zone enumeration.)

Validating responses. The resolver validates the response by

1. using the public VRF key in the NSEC5KEY record to validate that proof π from the NSEC5PROOF corresponds to the query α,
2. using a simple operation (*i.e.,* hashing) to get β from π and then checking that β falls between the two hash values in the NSEC5 record, and
3. using the public ZSK to validate the DNSSEC signatures on the NSEC5 record.

3.3 Properties of NSEC5.

Table 1 summarizes the properties of NSEC5.

[4]We use VRFs where β can be publicly computable from the proof π, so do not include β in the NSEC5PROOF record. VRFs that do not have this property additionally require β to be included in the NSEC5PROOF.

	integrity	privacy
Online signing	X	X
NSEC5	✓	X

Table 2: Comparing online signing (*e.g.,* NSEC3 White Lies) to NSEC5 when the nameserver is compromised.

Online crypto. NSEC5 requires online cryptographic computations for negative responses. (But not for positive responses.) For every query α that elicits a negative response, the nameserver uses the secret VRF key SK to compute the NSEC5PROOF record on the fly. Notice that online signing (*e.g.,* 'NSEC3 White Lies', see Section 2) also requires online cryptographic computations. The fact that both of these solutions prevent zone enumeration is not a coincidence: [40] proved that any solution that both (a) prevents zone enumeration and (b) provides weak integrity, must *necessarily* use online cryptography. What is interesting about NSEC5 is that it provides strong integrity (*i.e.,* integrity even when the nameserver is malicious or compromised). Meanwhile, online signing provides only weak integrity (*i.e.,* against network attackers but not compromised nameservers). See Tables 1-2.

Privacy. An attacker can only enumerate the zone by brute force—by sending an *online* query to the nameserver for each name α that it suspects is in the zone.

To see why, suppose an adversary has collected all the NSEC5 records for the zone, and now wants to enumerate the zone using an offline-dictionary attack that 'cracks' the VRF hashes. The adversary must first hash each entry in his dictionary, and then check if any of the hashed dictionary entries match any VRF hashes in the collected NSEC5 records; if there is a match, the adversary has successfully cracked the VRF hash. However, because the adversary does not know the private VRF key, the VRF hash values are indistinguishable from random values. It follows that the adversary cannot hash any of the entries in its dictionary, and thus cannot perform a offline dictionary attack. A formal security proof of this property is in [57].

Strong integrity. Strong integrity is provided even even if a malicious nameserver, or any other adversary, knows the secret VRF key SK. This is because because the untrusted nameserver does not know the secret zone-signing key (ZSK). The idea behind the formal proof (see [57]) of this property is simple. Suppose that the secret VRF key SK used with NSEC5 is made public. Resolvers know the correct public VRF key PK, so the VRF's trusted uniqueness ensures that an adversary (that knows SK) cannot trick resolvers into accepting an incorrect VRF hash output.[5] Then, NSEC5 is essentially the same as (plain) NSEC3: the adversary can correctly hash queries on its own, but cannot forge NSEC* records. Thus, for any name α that is present in the zone, the adversary cannot forge an NSEC5 record that falsely claims that α is absent from the zone. In other words, even if the private NSEC5KEY is leaked to an adversary, the security of NSEC5 just downgrades to that of (plain) NSEC3. (See Tables 1-2.)

3.4 An RSA-based VRF for NSEC5.

The original NSEC5 construction [40] was not described in terms of VRFs. However, it actually uses the VRF in Figure 1, which is based on RSA in the random oracle model (we provide the proof of the VRF properties in Appendix C).

Instantiation. Each precomputed NSEC5 record will contain two SHA-256 hash outputs, each corresponding to β in Figure 1, and one DNSSEC signature. Each NSEC5PROOF record, generated on the fly, has one RSA value (π in Figure 1).

3.5 An Elliptic Curve VRF for NSEC5.

We now see how to produce shorter NSEC5 responses using elliptic curves (EC). We use a VRF construction implicit in [33,38]. This VRF operates in a cyclic group G of prime order with generator g. The security of this VRF is proven in the random oracle model, and rests on the *decisional Diffie-Hellman (DDH)* assumption, which roughly says that h^x looks random given the tuple (g, g^x, h). Also, because [33,38] did not prove that this construction is a VRF, we provide new formal proofs that this construction satisfies the requirements of a VRF in Appendix B.

The construction is in Figure 2 and can be instantiated over any group where the decisional Diffie-Hellman (DDH) problem is hard, including the elliptic curves currently standardized in DNSSEC (NIST P-256 [46, Sec. 3]), and Curve25519 [51] which has recently been proposed for use with DNSSEC [48, 68]. Each of these curves achieves an approximately 128-bit security level [21, 46]. Both of these curves operate in finite field F_q, where q is a 256-bit prime.

[5]Notice that the trusted uniqueness property of the VRF is crucial for providing strong integrity. For the original RSA-based NSEC5 construction (Figure 1), trusted uniqueness follows because, for a given public key PK, the function $RSASIG_{SK}(MGF(\cdot))$ can produce exactly one proof value π for every input value α. Importantly, RSA signatures are unique given the public key PK but ECDSA signatures are not. This is why we cannot replace the RSA signature in Figure 1 with an ECDSA signature. With randomized ECDSA signatures, the signer uses a nonce as part of its signature computation, and so signatures are not unique given the ECDSA public key PK. Moreover, even deterministic ECDSA [64] fails to provide uniqueness given the ECDSA public key PK. This follows because with deterministic ECDSA, the signer derives the signing nonce from a keyed hash of the message it is signing, but the key k to this hash in *independent* of the ECDSA public key PK. Thus, PK does not allow the verifier to check that the signer used the correct nonce for each message it signed.

Keys. Let N be a public RSA modulus, let d be a secret RSA exponent and e be its corresponding public exponent. The public VRF key is (e, N) and the secret VRF key is (d, N).

Hashing. To hash input α using the private RSA key (d, N), start by computing the proof value

$$\pi = (MGF(\alpha))^d \mod N$$

and then compute the hash value β as

$$\beta = H(\pi)$$

H is a cryptographic hash function (*e.g.,* SHA-256) while MGF is an IETF-standard cryptographic hash that produces outputs one bit shorter than the RSA modulus [16, Sec. 10.2] (*aka,* a "full domain hash" [19]). Notice that anyone can compute β given π.

Verifying. To verify that β is the VRF hash of α, first verify that $H(\pi) = \beta$ and then use the public RSA key (e, N) to verify that π is a valid RSA signature on $MGF(\alpha)$, *i.e.,* that $\pi^e = MGF(\alpha) \mod N$.

Figure 1: A RSA-based VRF for NSEC5.

Instantiation. What response lengths do we get when we instantiate NSEC5 with the VRF in Figure 2 over 256-bit elliptic curves?

Each NSEC5 record will once again contain two hash outputs (each corresponding to β in Figure 2) along with a DNSSEC signature. We instantiate H_2 in Figure 2 with the function that outputs the x coordinate (abscissa) of a point (x, y) on the elliptic curve (where $x, y \in F_q$). Thus, each β will be 256-bits long.

We instantiate H_1 per Appendix A.

Next, observe that each NSEC5PROOF record will contain the proof value $\pi = (\gamma, c, s)$ from Figure 2. How long is π? If we instantiate the VRF using a 256-bit elliptic curve (*e.g.,* NIST P-256 or Ed25519), then s is 256 bits long. Meanwhile, γ is a point on the elliptic curve, which can be represented with $256 + 1$ bits using point compression.[6] Finally, we show (in Appendix B)

[6]The idea behind point compression is to represent a point with coordinates (x, y) using only its abscissa x (which is 256 bits long) and a single bit that indicates which square root (positive or negative) should be used for the ordinate y. Without point compression, both coordinates must be transmitted, for a total length of 256+256 bits. (Thus, without point compression our proof π would be $2 * 256 + 128 + 256 = 896$ bits long.) There has been some controversy over whether or not point compression is covered by a patent, and whether its use in DNSSEC corresponds to patent infringement [72]. However, as Bernstein [20] argues: "a patent cannot cover compression mechanisms [appearing in the paper by Miller in 1986 [55] that was] published seven years before the patent was filed." Moreover, new IETF specifications for elliptic curve digital signatures using Ed25519 also use point compression [48].

Public parameters. Let q be a prime number, Z_q be the integers modulo q, $Z_q^* = Z_q - \{0\}$, and let G a cyclic group of prime order q with generator g. We assume that q, g and G are public parameters of our scheme. Let H_1 be a hash function (modeled as a random oracle) mapping arbitrary-length bitstrings onto $G - \{1\}$. (See Appendix A for a suggested instantiation of H_1.) Let H_3 be a hash function (modeled as a random oracle) mapping arbitrary-length bitstrings to fixed-length bitstrings. We can use any secure cryptographic function for H_3; in fact, we need only the first ℓ bits of its output for ℓ-bit security. Let H_2 be a function that takes the bit representation of an element of G and truncates it to the appropriate length; we need a 256 bit output for 128-bit security.

Keys. The secret VRF key $x \in Z_q^*$ is chosen uniformly at random. The public VRF key is g^x.

Hashing. Given the secret VRF key x and input α, compute the proof π as:

1. Obtain the group element $h = H_1(\alpha)$ and raise it to the power of the secret key to get $\gamma = h^x$.
2. Choose a nonce $k \in Z_q$.
3. Compute $c = H_3(g, h, g^x, h^x, g^k, h^k)$.
4. Let $s = k - cx \bmod q$.

The proof π is the group element γ and the two exponent values c, s. (Note that c may be shorter than a full-length exponent, because its length is determined by the choice of H_3). The VRF output $\beta = F_{SK}(\alpha)$ is computed by truncating γ with H_2. Thus

$$\pi = (\gamma, c, s) \qquad \beta = H_2(\gamma)$$

Notice that anyone can compute β given π.

Verifying. Given public key g^x , verify that proof π corresponds to the input α and output β as follows:

1. Given public key g^x, and exponent values c and s from the proof π, compute $u = (g^x)^c \cdot g^s$.
   Note that if everything is correct then $u = g^k$.
2. Given input α, hash it to obtain $h = H_1(\alpha)$. Make sure that $\gamma \in G$. Use h and the values (γ, c, s) from the proof to compute $v = (\gamma)^c \cdot h^s$. Note that if everything is correct then $v = h^k$.
3. Check that hashing all these values together gives us c from the proof. That is, given the values u and v that we just computed, the group element γ from the proof, the input α, the public key g^x and the public generator g, check that:

$$c = H_3(g, H_1(\alpha), g^x, \gamma, u, v)$$

Finally, given γ from the proof π, check that $\beta = H_2(\gamma)$.

Figure 2: An EC-based VRF for NSEC5. We use a multiplicative group notation. This VRF adapts the Chaum-Pederson protocol [28] for proving that two cyclic group elements g^x and h^x have the same discrete logarithm x base g and h, respectively.

example.com	A
bar.example.com	A
www.example.com	A
*.www.example.com	A

Figure 3: Example zone.

c must be ℓ-bits long for an ℓ-bit security level. We therefore instantiate H_3 as the first 128 bits output by the SHA-256 hash function.

It follows that proof π will be $p = 256 + 1 + \ell + 256 = 513 + \ell$ bits for a ℓ-bit security level; thus, $p = 641$ for a 128-bit security level. Achieving the same security level with RSA requires 3072-bit RSA, which results in NSEC5PROOFS that are about 5 times longer!

4. DEALING WITH DNS WILDCARDS

Thus far, we have considered the operation of NSEC* in a very clean and idealized model, where every query ("What is the IP for `example.com`?") either elicits a positive response (*e.g.,* "172.18.216.34.") or a negative response ("NXDOMAIN: The name does not exist.") In practice, however, the behavior of NSEC* is much messier. This is primarily due to the complex nature of a seemingly-unrelated issue: DNS wildcards [52, Section 7.2.1], [37,53]. (Indeed, the treatment of DNS wildcards is so complex that RFC4592 [53] clarifying their use was issued nineteen years after the original DNS RFC1035 [56].) To properly understand how NSEC* performs in practice, we need to understand how each NSEC* scheme handles DNS wildcards. We then explain why these different approaches have significant implications on NSEC* performance, especially in terms of response length and computational overhead.

4.1 Wildcard and closest encloser proofs.

A wildcard record maps a set of queries to a particular response. For example, if the domain has a wildcard record for `*.example.com`, then queries for `c.example.com` and `a.b.c.example.com` would all be answered with the value in the wildcard record (*e.g.,* "172.18.216.35").

Wildcards have important implications for both NSEC3 and NSEC5. To see why, suppose a DNS query for `a.b.c.example.com` is made to the example zone in Figure 3. The correct response is NXDOMAIN (*i.e.,* the name does not exist). Why? First, `example.com` is the longest ancestor of the queried name that exists in the zone. In DNS terminology, `example.com` is the *closest encloser* for `a.b.c.example.com` [53]. Next, `*.example.com`—the wildcard child of the closest encloser—is not in the zone. Therefore, there is no *wildcard expansion* of query `a.b.c.example.com`. Thus, the correct response is NXDOMAIN.

But how can a nameserver use DNSSEC to securely *prove* the absence of relevant wildcards? First, the nameserver must prove that `example.com` is the closest encloser, by proving:

1. The presence of the *closest encloser* `example.com`.
2. The absence of the *next closer* `c.example.com`, the name one label longer than the closest encloser.

(Notice that the next closer is sometimes identical to the queried name, *e.g.,* if we had instead queried for `c.example.com`.) Once this is it done, the nameserver must additionally prove:

3. The absence of `*.example.com`, the wildcard child of the closest encloser.

How can NSEC* be used to prove the three items above? The middle and last item are easily dealt with, by providing the NSEC* recording proving the *absence* of the name, *i.e.,* that contains a pair of hashes h_1, h_2 such that $h_1 < h(\texttt{name}) < h_2$. But what about proving the *presence* of a name (*i.e.,* the first item)? One way to do this is to provide an NSEC* record that *matches* the name, *i.e.,* that contains a pair of hashes h_1, h_2 such that $h_1 = h(\texttt{name})$. Thus NSEC3 proves the three items by returning three NSEC3 records [52]:

1. A NSEC3 record *matching* the closest encloser, *i.e.,* an NSEC3 record with two hash values h_1, h_2 such that $h_1 = h(\texttt{example.com})$.
2. An NSEC3 record *covering* the next closer, *i.e.,* an NSEC3 record containing two hash values h_1, h_2 such that $h_1 < h(\texttt{c.example.com}) < h_2$.
3. An NSEC3 record *covering* the wildcard, *i.e.,* an NSEC3 record containing two hash values h_1, h_2 such that $h_1 < h(*.\texttt{example.com}) < h_2$.

Sometimes, fewer than three NSEC3 records are needed. For instance, only two records are needed if the same record matches $h(\texttt{example.com})$ and covers $h(\texttt{c.example.com})$. Indeed, this is *always* true for NSEC, so at most two NSEC records are returned for each query.

	online crypto at nameserver	verifications at resolver	max response length
NSEC	none	2 RRSIGs	2σ
NSEC3	none	3 RRSIGs	$3\sigma + 12\ell$
NSEC3 White Lies	1 RRSIG	3 RRSIGs	$3\sigma + 12\ell$
NSEC5	1 NSEC5PROOF	2 RRSIGs 2 NSEC5PROOFs	$2\sigma + 8\ell + 2p$

Table 3: Performance characteristics of NXDOMAIN responses for NSEC*. RRSIG records are DNSSEC signatures. σ is the bitlength of a DNSSEC signature, 2ℓ is the bitlength of the hash output in the NSEC3 or NSEC5 record, and p is the bitlength of an NSEC5PROOF.

4.2 Implications on NSEC3 performance.

Thus, wildcards significantly impact performance: a single query can solicit up to three NSEC3 responses! (Figure 4.)We now explain the impact on performance, which is also summarized in Table 3.

Response length. Every query can elicit a response containing (up to) three NSEC3 records, each of which includes as DNSSEC signature (of length σ bits) and two hash values (each of length 2ℓ bits). Thus, the bitlength of the response can be estimated as

$$|\text{nsec3}| = 3(4\ell + \sigma) = 12\ell + 3\sigma \quad (1)$$

Resolver computations. The resolver must verify up to three DNSSEC signatures (on each NSEC3).

Nameserver computations. When regular NSEC3 is used, all responses are precomputed, so the nameserver need not perform online public-key crypto computations. However, if NSEC3 White Lies is used, responses are generated on the fly, and up to three NSEC3 records must be signed in response to every query.

4.3 The wildcard bit.

In [37], however, Gieben and Mekking observed that wildcards could be dealt with just *two* NSEC3 records. Their proposal simply requires a *wildcard bit* to be added to each NSEC3 record. If an NSEC3 record contains the pair of hashes h_1, h_2 where $h_1 = h($`example.com`$)$, then the wildcard bit is set if `*.example.com` is present in the zone, and cleared otherwise. This simple trick allows us to eliminate the third NSEC3 record! Instead, we need only check that the wildcard bit is cleared on the first NSEC3 record. The wildcard bit was not standardized as part of NSEC3, and has not been deployed in practice [36]. However, we can use it with NSEC5, because NSEC5 records have the same structure as NSEC3 records.

4.4 Implications on NSEC5 performance.

NSEC5 uses the wildcard bit, so that up to two NSEC5 records (and two NSEC5PROOFs) are needed to respond to any query. (See Figure 5.)Table 3 summarizes the implications on NSEC5 performance.

Response lengths. Every query can elicit a response containing (up to) two NSEC5 records, each of which includes a DNSSEC signature (length σ bits) and two hash values (each of length 2ℓ bits), and up to two NSEC5PROOF records (each of length p bits). We can therefore estimate the total bitlength of the response as

$$|\text{nsec5}| = 2(4\ell + \sigma + p) = 8\ell + 2\sigma + 2p \quad (2)$$

Resolver computations. Resolvers need to verify two NSEC5PROOF records and up to two DNSSEC signatures (on NSEC5 records).

Nameserver computations. Recall that all DNSSEC signatures on NSEC5 records *must* be precomputed. (This is because NSEC5 records are signed by the zone-signing key (ZSK). To preserve strong integrity, the nameserver must not know the secret ZSK.)

But it is also possible to precompute one of the two NSEC5PROOFs. Specifically, the first NSEC5PROOF and NSEC5 record prove the presence of the closest encloser (*i.e.,* `example.com`) as follows: (1) The NSEC5 record has two hash values h_1, h_2, where h_1 is the VRF hash of the closest encloser, and (2) the NSEC5PROOF has a proof π that h_1 is a correct VRF hash value. The NSEC5PROOF for h_1 can therefore be computed and cached at the same time as the NSEC5 record.Online crypto is only needed for the second NSEC5PROOF. The second NSEC5PROOF and NSEC5 record *cover* the next closer `c.example.com`. The NSEC5PROOF proves that β is a correct VRF hash of `c.example.com`. Meanwhile, the NSEC5 record has a pair of VRF hash outputs h_1, h_2 that must fall lexicographically before and after β. Importantly, h_1 and h_2 must *not* equal β. Also, β is unknown at the time that the NSEC5 record is prepared. As such, the NSEC5PROOF for β cannot be precomputed.

Thus NSEC5 only needs one online cryptographic computation when the nameserver responds to a query.[7]

5. PRACTICAL CONSIDERATIONS

NODATA Responses. Thus far, our exposition has been a clean and idealized model where all DNS queries are of the same type: the query contains a domain name (`www.example.com`), and the response contains an IPv4 address ("172.18.216.34"). Actually, this is a query for an *A record*. In practice, there are other query types. For instance, the AAAA record is for IPv6 addresses. Suppose the example zone in Figure 3 receives a AAAA query for `www.example.com`. The zone has an A record for `www.example.com`, but not a AAAA one. Thus, the correct response is NODATA, (*i.e.,* "The name exists, but not for queried type").

Because NSEC5, NSEC3, and NSEC records all have the same structure, they all deal with NODATA responses as follows. Every NSEC* record includes a *type bitmap* [14, 52], containing a bit for each type of DNS record (*e.g.,* A, AAAA, NS, MX). Consider the NSEC* record matching `www.example.com`, *i.e.,* that contains a pair of hash values h_1, h_2 such that h_1 is the hash of `www.example.com`. In our example zone, this NSEC* record has its type A bit set, and its other type bits cleared. This NSEC* record would be used to respond to an AAAA query for `www.example.com`. The resolver would conclude the response is NODATA by checking that the the AAAA bit cleared. Notice that NODATA responses always use just one NSEC* record!

[7]As noted in Table 3, a similar precomputation approach is possible with NSEC3 White Lies. Specifically, the presence of the closest encloser `example.com` and the presence/absence of its wildcard child `*.example.com` are known at the time that the zone is signed. Therefore, their corresponding NSEC3 records can be precomputed. This optimization is (sort of) performed by the PowerDNS nameserver, which caches and reuses NSEC3 records generated on-the-fly for the closest encloser and wildcard.

Opt-out, key rollover. Because NSEC5 is so similar in structure to NSEC3, it also supports other important optimizations and procedures developed for DNSSEC. For instance, NSEC5 supports opt-out in the same way as NSEC3 [52]. Moreover, the NSEC5KEY can be rolled over using the same procedure to roll a ZSK [50]: the new NSEC5KEY record is published, then old NSEC5 records are replaced by NSEC5 records computed using the new NSEC5KEY, and finally the old NSEC5KEY is removed from the zone.

Privacy. Wildcards and types have only minor implications on NSEC5 privacy in practice.

Consider what happens when a queried name (*e.g.,* `a.b.c.example.com`) does not exist in the zone. Then, the NXDOMAIN response reveals the closest encloser's name (`example.com`) and types that exist in the zone (*e.g.,* A, AAAA, MX, NS), and also reveals if its wildcard child (`*.example.com`) exists in the zone. Meanwhile, if a queried name (*e.g.,* `www.example.com`) does exist in the zone, then the NODATA response reveals its all types (*e.g.,* A) present in the zone.

This means that NSEC5 ensures that an attacker can learn which types of a non-wildcard name (`example.com`) exist in the zone only if it (1) queries for the exact name (`example.com`) OR (2) queries for any longer name that contains it as a prefix (*e.g.,* `a.b.c.example.com`). In other words, the attacker must still enumerate the zone by brute force, sending an online query for every name (or longer name that contains it as a prefix) suspected to be in the zone.

6. IMPLEMENTATION

We designed and implemented the two NSEC5 variants (RSA and ECC), extending existing DNS software. For the authoritative nameserver, we extended Knot DNS 1.6.4, a highly-optimized authoritative implementation. For the recursive resolver we extended Unbound 1.5.9, one of the most widely used recursive resolver implementations. Our implementation supports the full spectrum of negative responses, (*i.e.,* NXDOMAIN, NODATA, Wildcard, Wildcard NODATA, and unsigned delegation). The authoritative implements the optimization that precomputes the NSEC5PROOFs matching each NSEC5 record (Section 4.4). We did not introduce additional library dependencies; all cryptographic primitives are already present in OpenSSL v1.0.2j, which is used by both implementations. We implemented our elliptic-curve VRF for the NIST P-256 curve. The code is deliberately modular, so that the Ed25519 curve [48] (which is not supported by OpenSSL v1.0.2j) could be used a drop-in replacement. Overall, we added approximately 9,000 lines of C code. We plan to make the source publicly available.

A "live" example from our implementation. Figures 4 and 5 present a NXDOMAIN response with NSEC3 and NSEC5 respectively. (Cryptographic values (hashes, proofs, and signatures) have been shortened and some data fields have been dropped.) We signed a "small" `example.com` zone with NSEC3 using ECDSA-P256 (DNSSEC algorithm 13) and ECC-based NSEC5. Per Section 4.2, NSEC3 returns three records and their corresponding signatures. On the other hand, the wildcard bit used with NSEC5 allows us to return only two NSEC5 records and two NSEC5PROOFS (Section 4.4).

```
$ kdig +dnssec +multiline ddadasds.example.com
;; ->>HEADER<<- opcode: QUERY; status: NXDOMAIN; id: 22793
;; Flags: qr aa rd; QUERY: 1; ANSWER: 0; AUTHORITY: 8; ADDITIONAL: 1

;; QUESTION SECTION:
;; ddadasds.example.com.  IN A

;; AUTHORITY SECTION:
example.com.     3600 IN SOA dns1.example.com.
example.com.     3600 IN RRSIG SOA 13 2 3600 20170128184611
              ( 5134 example.com. nqiEgM+kVBDeBI== )

;; Matching record for hash of example.com --closest encloser;
0sc7qshrek878fcmnag1.example.com. 3600 IN NSEC3 1 0 0 AABB
              ( CPDHD7GK40NGDKRU8CQ8 NS SOA MX RRSIG DNSKEY NSEC3PARAM )
0sc7qshrek878fcmnag1.example.com. 3600 IN RRSIG NSEC3 13 3 3600
              ( 5134 example.com. 2JicIoTH3WkgAjbP/ehmTv== )

;; Covering record for hash of ddadasds.example.com --next closer record;
jftj44t4kqppke20mukr.example.com. 3600 IN NSEC3 1 0 0 AABB
              ( MSC7QSHREK878FCM8GD7 A AAAA RRSIG )
jftj44t4kqppke20mukr.example.com. 3600 IN RRSIG NSEC3 13 3 3600
              ( 5134 example.com. VfFQfho5sQ8QVWOqsrXyN6== )

;; Covering record for hash of *.ddadasds.example.com --wildcard record;
cpdhd7gk40ngdkru8cq8n.example.com. 3600 IN NSEC3 1 0 0 AABB
              ( J1VSBFDBU38SMLNJPIMM A AAAA RRSIG )
cpdhd7gk40ngdkru8cq8n.example.com. 3600 IN RRSIG NSEC3 13 3 3600
              ( 5134 example.com. lcDsoeVGuq3rvezN2oW74x== )

;; Received 773 B
```

Figure 4: A typical NXDOMAIN response with NSEC3.

```
$ kdig +dnssec ddadasds.example.com
;; ->>HEADER<<- opcode: QUERY; status: NXDOMAIN; id: 18282
;; Flags: qr aa rd; QUERY: 1; ANSWER: 0; AUTHORITY: 8; ADDITIONAL: 1

;; QUESTION SECTION:
;; ddadasds.example.com.    IN A

;; AUTHORITY SECTION:
example.com.    3600 IN SOA dns1.example.com.
example.com.    3600 IN RRSIG SOA 16 2 3600
             ( 5137 example.com. kVfd4pgDmWMg== )

;; Matching record for hash of example.com --closest encloser;
;; Wildcard flag is not set;
ec2i1k1adn16bb9sbh1k.example.com. 86400 IN NSEC5 48566 0
             ( H4ETTRT2RNLVQA2DU6HM NS SOA MX RRSIG DNSKEY NSEC5KEY )
ec2i1k1adn16bb9sbh1k.example.com. 86400 IN RRSIG NSEC5 16 3 86400
             ( 5137 example.com. RbkKnf4MT/Fg== )

;; Covering record for hash of ddadasds.example.com --next closer record;
4vulla22dr6bo63j203c.example.com. 86400 IN NSEC5 48566 0
             ( C341KKJADV09N1BH2DJ0 A AAAA RRSIG )
4vulla22dr6bo63j203c.example.com. 86400 IN RRSIG NSEC5 16 3 86400
             ( 5137 example.com. KMrN9N+J9Rug== )

;; NSEC5PROOF records;
example.com.  3600 IN NSEC5PROOF 48566 ( AiZnaTPduKWyig )
ddadasds.example.com.  3600 IN NSEC5PROOF 48566 ( AzH6uKGjS+2FJf )

;; Received 834 B
```

Figure 5: A typical NXDOMAIN response with NSEC5.

7. PERFORMANCE EVALUATION

We now evaluate the performance of NSEC5 and compare it against (plain) NSEC3 and online signing with NSEC3 White Lies (Section 2). We consider response length, query processing time at the recursive

resolver and authoritative nameserver, and throughput, memory and CPU usage at the authoritative.

Configurations. We tested our Knot DNS nameserver implementation in four configurations:

1. NSEC3 with 2048-bit RSA signatures (DNSSEC Algorithm 8),
2. NSEC3 with ECDSA signatures over the NIST P-256 curve (DNSSEC Algorithm 13),
3. NSEC5 with 2048-bit RSA signatures (RRSIG) and NSECPROOF records,
4. NSEC5 with ECC using the NIST P-256 curve for both signatures (RRSIG) and NSECPROOFs.

The NSEC3 configurations used 10 hash iterations. (This is a common choice in practice, *e.g.,* at the `.ru` zone.) Finally, we used PowerDNS[8] 4.0.1 in "narrow" mode with BIND back-end to evaluate

5. NSEC3 White Lies with ECDSA signatures over NIST P-256 (DNSSEC Algorithm 13)

For the recursive resolver, we used our NSEC5-ready extension of Unbound in validating and caching mode.

Zone. We test against a real Alexa-100 second-level-domain (SLD) zone that consists of about 1000 names.

System. All experiments were executed on a machine with 20X Intel Xeon E5-2660 v3 cores with dual thread support for a total of 40 virtual CPUs, and 256GB RAM, running CentOS Linux 7.1.1503 and OpenSSL 1.0.2j. We would expect a typical SLD to have multiple nameservers of roughly this size, possibly at multiple locations. Because network latency is a common denominator for all our schemes, all experiments were performed with this machine hosting both the nameserver (using 24 threads) and the recursive resolver (using up to 16 threads), each listening at a different port.

Query load. Unless otherwise specified, our measurements use synthetic query loads. We elicit negative (NXDOMAIN) responses by sending queries for names from the zone prepended with a random six-alphanumeric-character sequence.

7.1 Response lengths.

We want DNSSEC responses to be short enough to fit into a single IP packet and to limit DDoS amplification (Section 1). Our measurements show that NSEC5-ECC response lengths are comparable to NSEC3 with ECDSA, and *shorter* than today's dominant deployment configuration (NSEC3 with 1024-bit RSA).

Figure 7. Figure 7 shows the average response size for 100,000 NXDOMAIN responses for our four Knot DNS configurations. When RSA is used, both NSEC5 (at 1731 bytes, on average) and NSEC3 (1517 bytes) do not fit in a 1500-byte IP packet (Ethernet MTU). Meanwhile, ECC-based NSEC5 is much shorter (827 bytes, on average), easily fitting into a single IP packet, and is comparable to ECC-based NSEC3 (783 bytes).

Comparison to "legacy" NSEC3. Modern cryptographic recommendations mandate a security level of at least 112 bits [17]. Despite these recommendations, NSEC3 only supports (outdated) SHA1 as its hash function [52], for an (outdated) security level of $\ell = 80$ bits. (NSEC5 records use a $2\ell = 256$-bit hash outputs, for a $\ell = 128$-bit security level.) Also, most domains deploying DNSSEC still use 1024-bit RSA ($\sigma = 1024$ bits) [69,74], for an (outdated) 80-bit security level [17]. NSEC3 with 1024-bit RSA has an average response length of 1069 bytes. This is about 29% *longer* than ECC-based NSEC5, which also has a much stronger security level ($\ell = 128$ versus $\ell = 80$ bits)!

7.2 Authoritative nameserver performance.

Both NSEC5, and online signing with NSEC3 White Lies, prevent offline zone enumeration by requiring online public-key crypto computations at the nameserver. (See Table 3.) We now compare performance at the nameserver, and find that our ECC-based NSEC5 implementation (extending Knot DNS) is *faster* than PowerDNS's implementation of NSEC3 White Lies.

Processing time per query. To measure the time it takes to process a query at the authoritative, we ran 100,000 sequential queries, each eliciting an NXDOMAIN response. To fairly compare across implementations, we report round-trip time as observed by the query issuer. Figure 6-(left) presents the results. Ignoring the tail of the plot (which can be attributed to delays in inter-process communication and other tasks running in the background), we see that the majority of queries are processed consistently close to an average time for each configuration. Plain NSEC3 (with RSA-2048 and

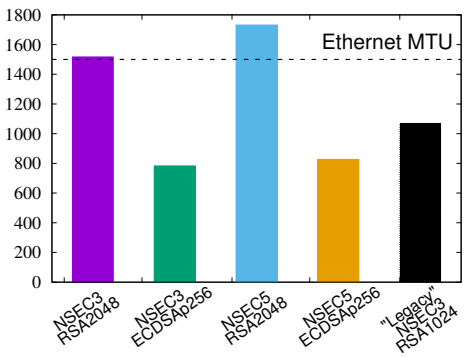

Figure 7: Average length for a single NXDOMAIN response (standard deviation $< 1\%$).

[8]We acknowledge that this is not an apples-to-apples comparison. But, to the best of our knowledge, PowerDNS is the only widely-deployed open-source nameserver that supports DNSSEC online signing in an RFC-compliant way. Meanwhile, we chose to focus our NSEC5 implementation effort on the more performant Knot DNS nameserver.

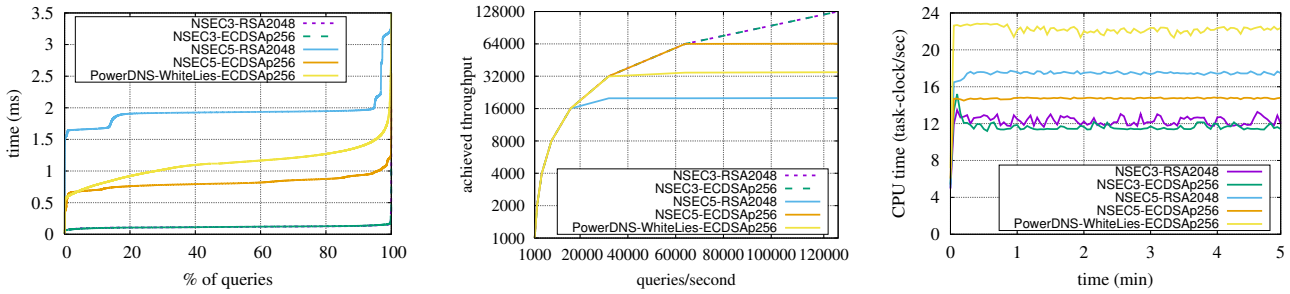

Figure 6: (Left) Query processing time at the authoritative nameserver per NXDOMAIN response. (Center) Throughput at the authoritative nameserver under stable query rate when all queries result in NXDOMAIN responses.(Right) CPU utilization (task-clock/second) for the different authoritative configurations at 32 Kqps query load and 24 threads.

ECDSA-P256) uses precomputed responses; as such, the nameserver can respond to queries in just 117μs and 116μs on average. Meanwhile NSEC5 and NSEC3 White Lies use online crypto, therefore process queries more slowly. RSA-based NSEC5 takes 1.93ms on average, while ECC-based NSEC5 presents a 2.3x speedup, for an average query processing time of 0.81ms. This is *faster* than the 1.12ms query processing time for the PowerDNS implementation of NSEC3 White Lies![9]

Throughput with negative traffic. Next, we consider aggregate query throughput. We used Dnsperf 2.1.1 [6], a popular open-source DNS performance evaluation tool, to issue negative queries at fixed rates from 1K to 128K queries per second (qps). Figure 6-(center) presents throughput results on a logarithmic scale.

Plain NSEC3 does not use online cryptographic computations, and so throughput scales easily to 128 Kqps and beyond. The remaining schemes do use online crypto computations. RSA-based NSEC5 plateaus earliest—the nameserver cannot cope with a query rate greater than about 20 Kqps. Turning to elliptic-curve configurations, PowerDNS's NSEC3 White Lies plateaus at about 32 Kqps, while our ECC-based NSEC5 improves on this to almost 64 Kqps. This 2x improvement follows from differences in the Knot DNS and PowerDNS implementations, which is also in line with benchmark results of [4]. ([4] finds a 2-3x gap in throughput between the Knot DNS and PowerDNS when serving DNSSEC-enabled zones.)Our NSEC3-ECC throughput results should be well above the needs of most zone operators. To put this in context, the A operator [1] reports an average negative query load per server that is roughly one order of magnitude smaller.

Throughput with mixed traffic. In practice, throughput should be even higher, because normal traffic should elicit positive responses (*e.g.,* signed A records), which are precomputed, in addition to NXDOMAIN responses. To demonstrate this, we tested ECC-based NSEC5 at a steady query rate of 32 Kqps using 4 (rather than 24) threads. When fewer than 50% of responses are NXDOMAIN, throughput remains steady at 32 Kqps. Meanwhile, purely NXDOMAIN traffic saturates throughput at 13 Kqps.

CPU utilization. CPU utilization is shown in Figure 6-(right). We used the Linux `perf_events` profiler to measure the `task-clock` time per second (shown on the y-axis of Figure 6-(right)), which reports the CPU time spent by a process across all threads. Since we use 24 threads, full utilization would correspond to a task-clock/second of 24. All measurements were taken over a 5 minute period (time shown on the x-axis) with 32 Kqps query load of purely NXDOMAIN traffic. From Figure 6-(center), we already know that a 32 Kqps query load causes throughput to deteriorate for RSA-based NSEC5 and PowerDNS's NSEC3 White Lies, but not for plain NSEC3 and ECC-based NSEC5. Considering the corresponding CPU utilization in Figure 6-(right), we see that plain NSEC3 has the lowest CPU utilization (roughly 50%, or `task-clock` time/second of about 12) while NSEC3-ECC is not too much higher. Meanwhile, NSEC3 White Lies (with PowerDNS) has the heaviest CPU utilization (roughly 95%, or `task-clock` time/second of about 23), mostly due to implementation differences between Knot DNS and PowerDNS. As a final note, we expect utilization to be lower in a setting tuned for maximum performance, since these results include the heavy logging necessary for our experiments.

[9]Per footnote 7, PowerDNS caches and reuses NSEC3 records generated on-the-fly for the closest encloser and wildcard. By contrast, our NSEC5 implementation *precomputes* the closest-encloser records, rather than caching and reusing them. Thus, to fairly compare across implementations, we crafted the query load so that all queries could use the same records (served from cache) for all but the next-closer records (Section 4.1). Therefore, both NSEC5-ECC and NSEC3 White Lies perform a single online crypto computation at query time.

	unsigned DNS	NSEC3 RSA2048	NSEC3 ECDSAp256	NSEC5 RSA2048	NSEC5 ECDSAp256	PowerDNS-WL ECDSAp256
tested SLD	18.1	49.3	43.9	64	53.3	18.6
`.name` TLD	108.3	417.2	254.7	634.1	492.2	144.4

Table 4: Memory footprint (MB) at the authoritative after loading the zone.

Memory footprint. Table 4 considers the memory footprint at the authoritative nameserver, once the zone is loaded. Because our test SLD zone had only 1000 records, we repeated this experiment for the `.name` TLD, which has about 460,000 records. We see that ECC generally has a much smaller memory footprint than RSA. NSEC5 also takes up more space than plain NSEC3 because: (i) NSEC5PROOFs are precomputed and cached to optimize performance (Section 4.4), and (ii) NSEC5 records use 256-bit hash values, while NSEC3 uses (outdated, less secure) 160-bit SHA1 hash values. Finally, the memory overhead for NSEC3 White Lies is tiny, because NSEC3 records are computed on the fly at query time.

7.3 Recursive resolver performance.

NSEC3 and NSEC5 both require recursive resolvers to perform public-key crypto verifications (Table 3). We therefore find that query processing times at the recursive resolver for our RSA- and ECC-based NSEC5 implementations are comparable to those of NSEC3.

Overall per-query processing time. Figure 8-(left) reports the overall query processing time per NXDOMAIN response, as observed by a stub resolver. This measurement includes the processing time both at the recursive resolver (which verifies DNSSEC responses) and at the authoritative nameserver (with serves or generates responses). We set up the stub resolver, recursive resolver, and nameserver on our single machine. Our query load was 100,000 sequential unique queries, each eliciting an NXDOMAIN response from the authoritative nameserver.

Figure 8-(left) shows that plain NSEC3, NSEC3 White Lies, and NSEC5 all have processing times of the same order of magnitude. This follows because they all require public-key crypto verifications at the recursive resolver. (Compare this to processing time at the authoritative nameserver alone, which is orders of magnitude faster for plain NSEC3). Naturally, overall processing time for plain NSEC3 is fastest (about 1ms); again, this follows because plain NSEC3 does not require online crypto at the authoritative nameserver. Of the three configurations that use online crypto at the nameserver to prevent zone enumeration, RSA-based NSEC5 takes the longest (3.4ms on average), followed by NSEC5-ECC (3.1ms on average) and NSEC3 White Lies using PowerDNS (2.4ms on average).

Mixed traffic. The average query processing time is likely to be faster in practice, since real DNSSEC traffic contains positive responses (*e.g.,* signed A records) as well as NXDOMAIN responses. To highlight this, Figure 8-(center) shows the overall query processing time for ECC-based NSEC5, when handling traffic containing both positive and NXDOMAIN responses. Positive queries were sampled from the zone according to a Zipf distribution, which has been shown to be a good fit for DNS query distributions [49]. Naturally, NSEC5 only affects performance for negative queries; everything else is validated from cache in minimal time.

Validation time. Finally, we zoom in on performance at the recursive resolver by considering only the time required for validating responses. (This excludes processing at the nameserver, latency to the nameserver, packet processing at the recursive, *etc.*).

Figure 6-(right) shows that cryptographic validation NSEC5-RSA is faster than NSEC5-ECC. (This is natural: RSA verification is well known to be faster than ECDSA verification.)

Next, consider the two plain NSEC3 configurations. Figure 6-(center) shows that most queries are validated in microseconds; meanwhile, the top 11% of queries (on the right side of the figure) take seconds to validate. The reasoning for this subtle. Because we issue 100,000 queries for a zone that only has 1000 names, our recursive resolver eventually collects all the NSEC3 records for the zone. (In other words, it enumerates the zone.) Once this happens, the authoritative nameserver begins sending NSEC3 records that the recursive resolver has already cached. Instead of cryptographically validating these NSEC3 records from scratch, the resolver simply takes a few microseconds to retrieve the cached NSEC3 record. Thus, the excellent validation performance of plain NSEC3 follows because we make a large number of queries to the same small zone. In a live system that queries multiple zones, this behavior is likely to be less significant.

Now consider the validation performance for NSEC3 White Lies. With White Lies, a fresh NSEC3 record is generated for every query, so the recursive will never be able to collect all the NSEC3 records for the zone. (That is, will never be able to enumerate the zone unless it queries specifically for all names in it!) Thus, this excellent validation performance we observed for plain NSEC3 is not possible with NSEC3 White Lies. Analogous reasoning shows it is also not possible with any other approach that prevents zone enumeration, including NSEC5.

Thus, it is most sensible to compare NSEC5's validation performance to that of NSEC3 White Lies. Figure 8-(right) shows that validation for NSEC3 White-

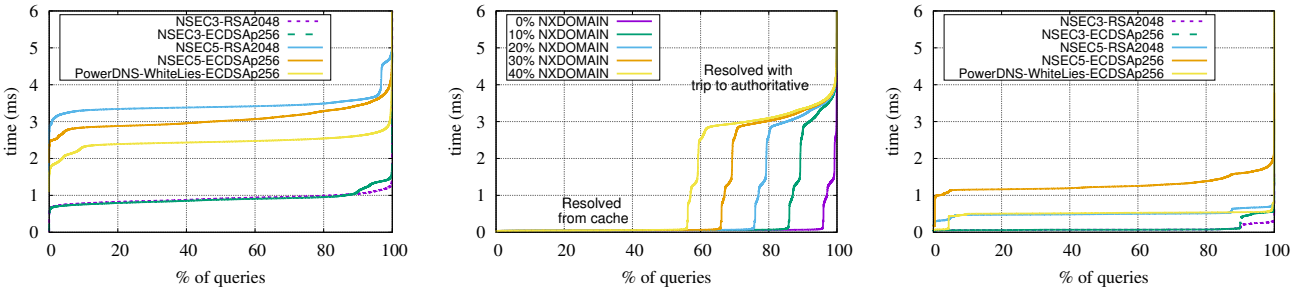

Figure 8: Overall query processing time at the recursive resolver and authoritative nameserver (left) per NXDOMAIN response across all configurations, and (center) for ECC-based NSEC5 under mixed (positive & NXDOMAIN) traffic. (right) Validation time per NXDOMAIN response at the recursive resolver for all configurations.

Lies (0.5ms) is faster than for NSEC5-ECC implementation (1.2ms). Digging into this result, we found that it is due to (1) parsing and logging the different parts of the NSEC5 response (*e.g.,* the NSEC5PROOF), (2) fetching the NSEC5KEY, and (3) a performance gap between our (unoptimized) VRF verification and the highly-optimized OpenSSL verification of ECDSA.

8. NSEC5 VS. RECENT INNOVATIONS

We consider the relationship between NSEC5 and some recent DNS innovations.

Aggressive negative caching (draft-ietf-dnsop-nsec-aggressiveuse) [34]: A new proposal, that is in the process of being standardized, calls for *aggressive caching* of NSEC* records at resolvers. The idea is to reuse cached NSEC* records to answer queries that are *different* from the original query that elicited the NSEC* record. (The original DNSSEC specifications [15] do not allow this.) To see how this works, suppose the zone in Figure 3 used (plain) NSEC and suppose we sent a type A query for `foo.example.com`. The response would contain an NSEC record that (1) attests that no names exist between `bar.example.com` and `www.example.com`, and (2) has a type bitmap with the type A bit set and type AAAA, NS, MX, *etc.* bits cleared. Then, aggressive negative caching allows resolvers to use the cached NSEC record to infer that:

1. Other names covered by the NSEC record do not exist in the zone (NXDOMAIN for *e.g.,* `qqq.example.com`).
2. Other types matching the NSEC record do not exist in the zone (NODATA for `bar.example.com` for types *e.g.,* AAAA, NS, MX).

This first item treats offline zone enumeration as feature, rather than a bug. In other words, it exploits the fact that resolvers can make offline inferences about the names covered by an NSEC/NSEC3 record. It optimizes DNSSEC performance by cutting down on the number of queries sent from resolver to nameserver. (For instance, the fast response validation behavior we observed for plain NSEC3 in Figure 8-(right) would also translate to a reduce number of queries.) However, this performance optimization is obviated by *any* scheme that prevents offline zone enumeration, including NSEC3 White Lies and NSEC5, because these schemes *necessarily* prevent resolvers from making offline inferences about the names present or absent in the zone. Meanwhile, the second item optimizes performance (reducing queries from resolver to nameserver) for all the schemes including NSEC5.

RFC8020 [25]. RFC8020 is a new standard that states that NXDOMAIN for a query (`c.example.com`) implies that names deeper in the DNS hierarchy (*e.g.,* `b.c.example.com`) also do not exist. This allows resolvers to cache the NXDOMAIN response for `c.example.com` and reuse it to answer a later query for *e.g.,* `b.c.example.com`. All the NSEC* variants we have considered thus far, including NSEC5, can benefit from this performance optimization.

Black Lies (draft-valsorda-dnsop-black-lies [70]). There is a (concurrent) NSEC* proposal that leverages the fact that NODATA responses are short. Black Lies is an online-signing solution that answers each negative query with an NODATA response, even if the "correct" response is NXDOMAIN. (Hence, the Black Lie.) For example, suppose the zone in Figure 3 receives an AAAA query for `a.example.com`. The Black Lies response is a single NSEC record matching `a.example.com`, with its AAAA type bit cleared, that is generated and signed on the fly. To prevent zone enumeration, the second name in the NSEC record is the immediate lexicographic successor of query, *i.e.,* `\000.a.example.com`. Only one NSEC record is required, so Black Lies responses are short.

Black Lies comes with some caveats. First, it is an online-signing solution (per Tables 1,2) that requires the nameserver to know the secret zone-signing key (ZSK). Thus, it fails to provide strong integrity. Second, because Black Lies gives a NODATA response when the "correct" response is NXDOMAIN, it obviates

the performance optimization of RFC8020 [25]. Also, Black Lies thwarts any diagnostic or security tool (*e.g.,* [31, 65]) that uses NXDOMAIN responses to infer that a name definitely does not exist in the zone.

9. SUMMARY: WHY USE NSEC5?

The key advantage of NSEC5 is that it (1) stops offline zone enumeration while (2) providing integrity even if the zone's authoritative nameserver is compromised. By contrast, DNSSEC's online signing solutions (NSEC3 White Lies [36], Minimally-Covering NSEC [77], Black Lies [70]) stops offline zone enumeration by trusting the nameserver with the secret zone-signing key (ZSK); thus compromising the nameserver compromises the integrity of the zone.

[40] proved that providing integrity and preventing offline zone enumeration *necessarily* require the nameserver to perform one online public-key crypto computation for each negative query. While this seems expensive, we demonstrate that our ECC-based NSEC5 nameserver implementation can be viable even for high-throughput scenarios. In Section 7.2 we found that it supports a throughput of 64,000 negative queries per second (qps) on a moderately-sized server with 24 threads on 40 virtual cores. This is about 2x the throughput of the only implementation of RFC-compliant online signing that is widely deployed and publicly available (PowerDNS's implementation of NSEC3 White Lies). A throughput of 64 Kqps should be well above the needs of most zone operators—even public statistics from the A-root operator [1] indicate an average negative query load about one order of magnitude smaller per server. Without access to proprietary statistics regarding corporate second-level-domains, it is not easy to estimate their throughput requirements. Nevertheless, this 64 Kqps throughput is achieved even with purely negative traffic (rather that mixed traffic, with both positive and negative queries) and a single server (rather than a cluster of nameservers, a more common deployment configuration).

With ECC-based NSEC5, the overall processing time for an negative query (from stub resolver, to recursive resolver, to authoritative nameserver) is only 30% longer that of online signing with NSEC3 White Lies (using the PowerDNS implementation). It may be possible to reduce this performance gap with an optimized implementation, since the nature and number of cryptographic operations in the two configurations is similar.

Thus, we believe that NSEC5 can be a practical solution for zone operators that care about protecting sensitive information (names of hosts, servers, routers, IoT devices, DANE certificates [45], *etc.*) from offline zone enumeration attacks. Meanwhile, operators that don't care about zone enumeration should just use plain NSEC3. Moreover, for zones that currently use online signing with NSEC3 White Lies, moving to NSEC5 seems like a win-win scenario: roughly the same (if not better) performance, and no need to store the sensitive secret ZSK at the authoritative nameserver.

10. THE TRANSITION TO NSEC5

We conclude with a discussion of the elephant in the room. How can today's DNSSEC transition to NSEC5?

The DNS community has faced this problem before. First, the NSEC3 specification [52] came out after the earliest deployments of DNSSEC [59], and so resolvers and nameservers had to transition from NSEC to NSEC3 [52, Section 10.4]. Second, there is currently a proposal to transition from RSA to ECDSA signatures over the NIST P-256 elliptic curve [72]. Third, a desire to avoid NIST-specified curves [23] and to have short DNSSEC responses, is motivating the community to consider transitioning to digital signatures over Edwards elliptic curves [68, 79]. Fourth, there is also the DPRIVE initiative that seeks to add confidentiality to DNS transactions, to mitigate concerns surrounding pervasive network monitoring [11]. Given that other transitions may be on the horizon, this might also be a good time to consider transitioning to NSEC5.

10.1 The mechanics of the transition.

We believe that the transition to NSEC5 can be accomplished similarly to the transition to NSEC3. DNSSEC records have an *algorithm number* that specifies the cryptographic algorithms they use (*e.g.,* 5 specifies RSA signatures with SHA1 hashing [47]). To transition to NSEC3, two new algorithm numbers were introduced—6:DSA-NSEC3-SHA1 and 7:RSASHA1-NSEC3-SHA1. (Once the transition period ended, subsequent DNSSEC algorithm numbers (8,10, 12, *etc.*) implied support of NSEC3.) Per [15, Sec 5.2], resolvers that did not support NSEC3 ignored DNSSEC records with algorithms 6 or 7, and either 'hard failed' (*i.e.,* rejected the response) or 'soft failed' (*i.e.,* accepted the response) depending on their local policies.

New algorithm numbers could also be used to transition to NSEC5. There are two ways [50, Sec 4.1.4] to transition from an old algorithm number to a new one.

1. Conservative approach. The nameserver simultaneously supports both algorithms. Thus, the nameserver answers each query with a DNSSEC response has records for both the old and the new algorithm number. The resolver can validate the response if recognizes at least one algorithm. The downside is that DNSSEC responses contain twice as many keys and signatures.

2. Liberal approach. Here, the nameserver stops serving responses with the old algorithm, and use the new algorithm instead. The downside is that resolvers that do not support the new algorithm number will treat the zone as unsigned [15, Sec 5.2]. As such, the liberal

approach is unlikely to be used until the majority of resolvers support the new algorithm number.

There are several reasons why the liberal approach seems right for NSEC5. First, it does not blow up the length of DNSSEC responses. Secondly, and more importantly, a zone that simultaneously supports both NSEC3 and NSEC5 will not reap the security benefits of NSEC5. If (plain) NSEC3 is supported in parallel with NSEC5, then offline zone enumeration is possible by collecting the NSEC3 records.[10] If online signing (*e.g.,* NSEC3 White Lies) is supported in parallel with NSEC5, then the nameserver must hold the secret ZSK key, and thus NSEC5 loses its strong integrity guarantees. On the other hand, the liberal approach is unlikely to be used in a transition until a majority of resolvers support NSEC5. However, given that resolvers might soon be upgraded to add support for Edwards curves, now might also be a good time to consider adding support for NSEC5.

Acknowledgements

We thank innumerable DNS practitioners for pushing us to develop a more performant version of NSEC5. We also thank Asaf Ziv, Sachin Vasant, Ondrej Sury and Tomofumi Okubo for earlier collaborations on NSEC5. This research was supported, in part, by NSF grants 1012798, 1012910 and 5245250 and a gift from Verisign Labs.

11. REFERENCES

[1] A Root server raw data. http://a.root-servers.org/raw-data/index.html.
[2] Kali Tools: DNSRecon. http://tools.kali.org/information-gathering/dnsrecon.
[3] Knot DNS. https://www.knot-dns.cz/.
[4] Knot DNS: Benchmark. https://www.knot-dns.cz/benchmark/.
[5] nmap: dns-nsec-enum. https://nmap.org/nsedoc/scripts/dns-nsec-enum.html.
[6] Nominum Measurement Tools. http://www.nominum.com/measurement-tools/.
[7] nsec3map: John the Ripper plugin. https://github.com/anonion0/nsec3map.
[8] PowerDNS. https://www.powerdns.com/.
[9] Microsoft security bulletin ms11-058 - critical: Vulnerabilities in dns server could allow remote code execution (2562485). https://technet.microsoft.com/library/security/ms11-058, August 9 2011.
[10] The heartbleed bug. http://heartbleed.com/, 2014.
[11] DNS PRIVate Exchange Working Group Charter (DPRIVE), 2015. https://datatracker.ietf.org/doc/charter-ietf-dprive/.
[12] Microsoft security bulletin ms15-127 - critical: Security update for microsoft windows dns to address remote code execution (3100465). https://technet.microsoft.com/en-us/library/security/ms15-127.aspx, December 8 2015.
[13] B. Aitken. Interconnect communication MC / 080:DNSSEC Deployment Study. http://stakeholders.ofcom.org.uk/binaries/internet/domain-name-security.pdf, 2011.
[14] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. *RFC 4034: Resource Records for the DNS Security Extensions*. Internet Engineering Task Force (IETF), 2005. http://tools.ietf.org/html/rfc4034.
[15] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. *RFC 4035: Protocol Modifications for the DNS Security Extensions*. Internet Engineering Task Force (IETF), 2005. http://tools.ietf.org/html/rfc4035.
[16] J. S. B. Kaliski. *RFC 2437: PKCS #1: RSA Cryptography Specifications, Version 2.0*. Internet Engineering Task Force (IETF), 1998. http://tools.ietf.org/html/rfc2437.
[17] E. Barker and Q. Dang. Recommendation for Key Management - Part 3 Application-Specific (Revised). NIST Special Publication 800-57.
[18] J. Bau and J. C. Mitchell. A security evaluation of dnssec with nsec3. In *NDSS*, 2010.
[19] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on Computer and communications security*, pages 62–73. ACM, 1993.
[20] D. J. Bernstein. Irrelevant patents on elliptic-curve cryptography. http://cr.yp.to/ecdh/patents.html (Accessed 1/15/2016).
[21] D. J. Bernstein. Curve25519: new Diffie-Hellman speed records. In *Public Key Cryptography-PKC 2006*, pages 207–228. Springer, 2006.
[22] D. J. Bernstein. Nsec3 walker. http://dnscurve.org/nsec3walker.html, 2011.
[23] D. J. Bernstein, T. Lange, and R. Niederhagen. Dual ec: A standardized back door. In *The New Codebreakers*, pages 256–281. Springer, 2016.
[24] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. In *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, pages 514–532, 2001.
[25] S. Bortzmeyer and S. Huque. *RFC 8020: NXDOMAIN: There Really Is Nothing Underneath*. Internet Engineering Task Force (IETF), 2005. http://tools.ietf.org/html/rfc8020.
[26] C. Boyd, P. Montague, and K. Nguyen. Elliptic curve based password authenticated key exchange protocols. In V. Varadharajan and Y. Mu, editors, *Information Security and Privacy*, volume 2119 of *Lecture Notes in Computer Science*, pages 487–501. Springer Berlin Heidelberg, 2001.
[27] M. Chase and A. Lysyanskaya. Simulatable vrfs with applications to multi-theorem NIZK. In *CRYPTO'07*, pages 303–322, 2007.
[28] D. Chaum and T. P. Pedersen. Wallet databases with observers. In *Advances in Cryptology-CRYPTO'92*, pages 89–105. Springer, 1992.
[29] J. Coron. On the exact security of full domain hash. In M. Bellare, editor, *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, volume 1880 of *Lecture Notes in Computer Science*, pages 229–235. Springer, 2000.
[30] J. Damas, M. Graff, and P. Vixie. *RFC 6891: Extension Mechanisms for DNS (EDNS(0))*. Internet Engineering Task Force (IETF), 2013. http://tools.ietf.org/html/rfc6891.
[31] C. Deccio. DNSviz: a tool for visualizing the status of a DNS zone. http://dnsviz.net/, 2010.
[32] D. Fisher. Final report on diginotar hack shows total compromise of ca servers. Threatpost. https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/, 2012.
[33] M. Franklin and H. Zhang. Unique ring signatures: A practical construction. In *Financial Cryptography and Data Security*, pages 162–170. Springer, 2013.
[34] K. Fujiwara, A. Kato, and W. Kumari. *draft-ietf-dnsop-nsec-aggressiveuse: Aggressive use of NSEC/NSEC3*. Internet Engineering Task Force (IETF), 2016. https://datatracker.ietf.org/doc/draft-ietf-dnsop-nsec-aggressiveuse.
[35] S. Gibson. Distributed Reflection Denial of Service (DrDoS) Attacks. Technical report, Gibson Research Corporation, 2002.
[36] R. Gieben and W. Mekking. *RFC 7129: Authenticated Denial of Existence in the DNS*. Internet Engineering Task Force (IETF), 2014. http://tools.ietf.org/html/rfc7129.
[37] R. Gieben and W. Mekking. draft-gieben-nsec4-00:DNS Security (DNSSEC) Authenticated Denial of Existence, 2015. http://tools.ietf.org/html/draft-gieben-nsec4-00.
[38] E. Goh and S. Jarecki. A signature scheme as secure as the diffie-hellman problem. In *Advances in Cryptology - EUROCRYPT 2003*, pages 401–415, 2003.
[39] S. Goldberg, M. Naor, D. Papadopoulos, and L. Reyzin. Nsec5 from elliptic curves. *ePrint Cryptology Report 2016/083* *http://eprint.iacr.org/2016/083.pdf*, 2016.
[40] S. Goldberg, M. Naor, D. Papadopoulos, L. Reyzin, S. Vasant,

[10] This also suggests that algorithm negotiation [42] may be less helpful in a transition to NSEC5—a zone-enumeration attacker can simply negotiate to speak NSEC3.

and A. Ziv. NSEC5: provably preventing DNSSEC zone enumeration. In *NDSS'15*, 2015. https://eprint.iacr.org/2014/582.pdf.
[41] A. Herzberg and H. Shulman. Fragmentation considered poisonous, or: One-domain-to-rule-them-all. org. In *Communications and Network Security (CNS), 2013 IEEE Conference on*, pages 224–232. IEEE, 2013.
[42] A. Herzberg and H. Shulman. Negotiating dnssec algorithms over legacy proxies. In *Proceedings of the 13th International Conference on Cryptology and Network Security - Volume 8813*, pages 111–126, New York, NY, USA, 2014. Springer-Verlag New York, Inc.
[43] A. Herzberg and H. Shulman. Cipher-suite negotiation for dnssec: Hop-by-hop or end-to-end? *Internet Computing, IEEE*, 19(1):80–84, 2015.
[44] S. Higginbotham. Anatomy of a hack: How the sea took down the nyt and twitter. https://gigaom.com/2013/08/27/anatomy-of-a-hack-how-the-sea-took-down-the-nyt-and-twitter/, August 27 2013.
[45] P. Hoffman and J. Schlyter. *RFC 6698: The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSAC*. Internet Engineering Task Force (IETF), 2012. http://tools.ietf.org/html/rfc6698.
[46] P. Hoffman and W. Wijngaards. *RFC 6605: Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC*. Internet Engineering Task Force (IETF), 2012. http://tools.ietf.org/html/rfc6605.
[47] IANA. Domain Name System Security (DNSSEC) Algorithm Numbers http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml.
[48] S. Josefsson and N. Moeller. draft-irtf-cfrg-eddsa: Edwards-curve Digital Signature Algorithm (EdDSA), 2016. https://datatracker.ietf.org/doc/draft-irtf-cfrg-eddsa.
[49] J. Jung, E. Sit, H. Balakrishnan, and R. Morris. DNS performance and the effectiveness of caching. In *Proceedings of the 1st ACM SIGCOMM Internet Measurement Workshop, IMW 2001*, pages 153–167, 2001.
[50] O. Kolkman, W. Mekking, and R. Gieben. *RFC 6781: DNSSEC Operational Practices, Version 2*. Internet Engineering Task Force (IETF), 2012. http://tools.ietf.org/html/rfc6781.
[51] A. Langley, M. Hamburg, and S. Turner. *RFC 7748: Elliptic Curves for Security*. Internet Engineering Task Force (IETF), 2016. http://tools.ietf.org/html/rfc7748.
[52] B. Laurie, G. Sisson, R. Arends, and D. Blacka. *RFC 5155: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence*. Internet Engineering Task Force (IETF), 2008. http://tools.ietf.org/html/rfc5155.
[53] E. Lewis. *RFC 4592: The Role of Wildcards in the Domain Name System*. Internet Engineering Task Force (IETF), 2006. http://tools.ietf.org/html/rfc4592.
[54] S. Micali, M. O. Rabin, and S. P. Vadhan. Verifiable random functions. In *FOCS*, pages 120–130. IEEE Computer Society, 1999.
[55] V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology (CRYPTO'85 Proceedings)*, pages 417–426. Springer, 1986.
[56] P. Mockapetris. *RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION*. Internet Engineering Task Force (IETF), 1987. http://tools.ietf.org/html/rfc1035.
[57] M. Naor and A. Ziv. Primary-secondary-resolver membership proof systems. In *Theory of Cryptography*, pages 199–228. Springer, 2015. https://eprint.iacr.org/2014/905.
[58] NLNetLabs. ldns. http://git.nlnetlabs.nl/ldns/tree/examples/ldns-walk.c.
[59] E. Osterweil, D. Massey, and L. Zhang. Observations from the dnssec deployment. In *The 3rd workshop on Secure Network Protocols (NPSec)*, 2007.
[60] E. Osterweil, D. Massey, and L. Zhang. Availability problems in the DNSSEC deployment, 2009. http://irl.cs.ucla.edu/talks/2009-05-RIPE-PMTU.pptx.
[61] E. Osterweil, D. Massey, and L. Zhang. Deploying and monitoring DNS security (DNSSEC). In *Twenty-Fifth Annual Computer Security Applications Conference, ACSAC 2009, Honolulu, Hawaii, 7-11 December 2009*, pages 429–438. IEEE Computer Society, 2009.
[62] E. Osterweil, D. McPherson, and L. Zhang. The shape and size of threats: Defining a networked system's attack surface. In *22nd IEEE International Conference on Network Protocols, ICNP 2014, Raleigh, NC, USA, October 21-24, 2014*, pages 636–641. IEEE Computer Society, 2014.
[63] E. Osterweil, M. Ryan, D. Massey, and L. Zhang. Quantifying the operational status of the DNSSEC deployment. In K. Papagiannaki and Z. Zhang, editors, *Proceedings of the 8th ACM SIGCOMM Internet Measurement Conference, IMC 2008, Vouliagmeni, Greece, October 20-22, 2008*, pages 231–242. ACM, 2008.
[64] T. Pornin. *RFC 6979: Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)*. Internet Engineering Task Force (IETF), 2013. http://tools.ietf.org/html/rfc6979.
[65] Root Server System Advisory Committee (RSSAC). RSSAC002: RSSAC Advisory on Measurements of the Root Server System. Technical report, ICANN, November 2014. https://www.icann.org/en/system/files/files/rssac-002-measurements-root-20nov14-en.pdf.
[66] M. Sanz. Dnssec and the zone enumeration. European Internet Forum: http://www.denic.de/fileadmin/public/events/DNSSEC_testbed/zone-enumeration.pdf, October 2004.
[67] M. Sivaraman, S. Kerr, and L. Song. *draft-muks-dns-message-fragments-00: DNS message fragments*. Internet Engineering Task Force (IETF), 2015. http://tools.ietf.org/html/draft-muks-dns-message-fragments-00.
[68] O. Sury and R. Edmonds. *draft-ietf-curdle-dnskey-ed25519: Ed25519 for DNSSEC*. Internet Engineering Task Force (IETF), 2016. https://datatracker.ietf.org/doc/draft-ietf-curdle-dnskey-ed25519/.
[69] L. Valenta, S. Cohney, A. Liao, J. Fried, S. Bodduluri, and N. Heninger. Factoring as a service. Cryptology ePrint Archive, Report 2015/1000, 2015. http://eprint.iacr.org/2015/1000.
[70] F. Valsorda and O. Gudmundsson. *draft-valsorda-dnsop-black-lies: Compact DNSSEC Denial of Existence or Black Lies (expired)*. Internet Engineering Task Force (IETF), 2016. https://datatracker.ietf.org/doc/draft-valsorda-dnsop-black-lies/.
[71] R. van Rijswijk-Deij, A. Sperotto, and A. Pras. DNSSEC and its Potential for DDoS Attacks: A Comprehensive Measurement Study. In *IMC'14*, pages 449–460. ACM, 2014.
[72] R. van Rijswijk-Deij, A. Sperotto, and A. Pras. Making the case for elliptic curves in dnssec. *ACM SIGCOMM Computer Communication Review*, 45(5):13–19, 2015.
[73] J. Vcelak, D. Papadopoulos, and S. Goldberg. draft-vcelak-nsec5:NSEC5, DNSSEC Authenticated Denial of Existence, 2015. https://datatracker.ietf.org/doc/draft-vcelak-nsec5.
[74] Verisign Labs. SecSpider: Global dnssec deployment tracking. http://secspider.verisignlabs.com/.
[75] M. Wander. nsec3breaker. https://www.vs.uni-due.de/trac/dnssec, 2016.
[76] M. Wander, L. Schwittmann, C. Boelmann, and T. Weis. GPU-Based NSEC3 Hash Breaking. In *IEEE Symp. Network Computing and Applications (NCA)*, 2014.
[77] S. Weiler and J. Ihren. *RFC 4470: Minimally Covering NSEC Records and DNSSEC On-line Signing*. Internet Engineering Task Force (IETF), 2006. http://tools.ietf.org/html/rfc4592.
[78] H. Yang, E. Osterweil, D. Massey, S. Lu, and L. Zhang. Deploying cryptography in internet-scale systems: A case study on DNSSEC. *IEEE Trans. Dependable Sec. Comput.*, 8(5):656–669, 2011.
[79] D. York, O. Sury, P. Wouters, and O. Gudmundsson. *draft-york-dnsop-deploying-dnssec-crypto-algs: Observations on Deploying New DNSSEC Cryptographic Algorithms*. Internet Engineering Task Force (IETF), 2016. https://datatracker.ietf.org/doc/draft-york-dnsop-deploying-dnssec-crypto-algs/.

APPENDIX

A. HASHING ONTO THE CURVE.

The VRF (Section 3.5) uses a hash function H_1 that maps arbitrary-length strings to points on an elliptic curve. How can we instantiate such a hash function? Ideally we want an instantiation that can work for both curves we have considered here: NIST P-256 and Curve25519.

One very lightweight technique was proposed in [24] and, at a high level, it proceeds as follows. Assume an elliptic curve with corresponding equation $y^2 =$

$x^3 + ax + b$ (in Weierstrass form). Given an integer α (the queried name in our case), set counter $i = 0$ and compute $h = H(\alpha||i)$, where H is a standard cryptographic hash function, *e.g.,* SHA-256, and $||$ is concatenation. Then, if $h^3 + ax + b$ is a quadratic residue (that is, h is the valid x-coordinate of a point on the curve) output $(h, (h^3 + ax + b)^{1/2})$. Otherwise, increment the counter by 1 and try again. This simple process is expected to terminate after two steps, and the involved operations are very fast, with an expected running time of $(O \log^3(q))$, if the curve is defined over finite field F_q. The range of this function is only half of the group G (because only one y is chosen for a random x), but that does not materially change the proofs of security (specifically, in Claims B.4 and B.5, the running time for simulating queries to H_1 doubles).

As first shown in [26], the above technique is not suitable when α must be kept secret; this is because the running time of the hashing algorithm depends on α, and so it is susceptible to timing attacks. However, we stress that this attack is not relevant in the context of NSEC5. The only value that is hashed in the query phase is the queried name α itself, which is already known to the adversary.

B. SECURITY PROOFS.

We define the necessary security properties that a VRF needs to satisfy in order to be used in our application, and provide formal proofs that our construction satisfies them.

B.1 Proof sketches.

We start with a sketch of the proofs of three properties: uniqueness, psuedorandomness, and collision resistance. We define and prove them formally after the brief informal sketch.

Uniqueness. The proof is by contradiction. Suppose an adversary, given the secret key x, can come up with some α and an incorrect VRF output value $\beta_1 \neq H_2([H_1(\alpha)]^x)$ for that α, and a valid proof $\pi_1 = (\gamma_1, s_1, c_1)$ for value β_1. The verification function for the VRF computes $h = H_1(\alpha)$ and

$$u = (g^x)^{c_1} g^{s_1}$$
$$v = (\gamma_1)^{c_1} h^{s_1}$$

Now take the logarithm of the first equation base g and the logarithm of the second equation base h, subtract the two resulting equations, and express c_1, to get

$$c_1 \equiv \frac{\log_g u - \log_h v}{x - \log_h \gamma_1} \pmod{q}. \qquad (3)$$

Now since $\gamma_1 \neq h^x$ (since β_1 is not the correct output value), the denominator is not zero, and there is exactly one c_1 modulo q that satisfies equation (4) for a given $(g, h, g^x, \gamma, u, v)$, *regardless* of s. However, recall that the verifier checks that c_1 is equal to the output of the cryptographic hash function H_3 on input $(g, h, g^x, \gamma, u, v)$. Since H_3 is a random oracle, its output is random, and the probability that it equals the unique value determined by its inputs according to (3) is negligible.[11] Thus, we have arrived at our contradiction.

Pseudorandomness. This follows from the DDH assumption, in the random oracle model. Roughly speaking, the pseudorandomness adversary does not know the secret VRF key x, but must distinguish between between pairs (α, β) where β is the VRF hash output on input α, and pairs (α, r) where r is a random value. This adversary knows the public values g and g^x, and can easily compute $h = H_1(\alpha)$ for any α. However, by the DDH assumption, h^x looks random even given (g, g^x, h), and so $H_2(h^x)$ is pseudorandom in the range of H_2.

Collision-Resistance. For a collision to happen, $H_2(h_1^x)$ should equal to $H_2(h_2^x)$ where $h_1 = H_1(\alpha_1)$ and $h_2 = H_1(\alpha_2)$ for some $\alpha_1 \neq \alpha_2$. Assume H_2 is a τ-to-1 function. Since raising to the power x is a permutation, for every h_1, there are at most τ possible h_2 values that can cause a collision. Since h_1 and h_2 are obtained via random oracle queries, a pair that causes a collision is unlikely to be found after Q_H queries to H_1, as long as G is larger than $\tau Q_H^2/2$.

B.2 Full Proofs

We now expand on the sketches above to prove that the construction in Section 3.5 is a secure VRF. It suffices to prove three properties: Trusted Uniqueness (see [57, Definition 10]), Selective Pseudorandomness (see [57, Definition 11]), and Collision-Resistance (not formally discussed in [57], but mentioned in the proof of Theorem 4). Sufficiency of these three properties for constructing NSEC5 follows from [57, Theorem 4]. We discuss each property in turn.

We model the hash functions H_1 and H_3 as random oracles. We use notation $\mathsf{Ver}_{PK}(\alpha, \beta, \pi)$ to denote the verification algorithm, which outputs 1 if and only if the proof π and hash output β are valid for input α and public key PK.

B.2.1 Uniqueness.

Recall that uniqueness requires that there should be only one provable VRF output β for every input α; *trusted* uniqueness limits this requirement to only the case when the public key is valid.

Following tradition of the VRF literature, Naor and Ziv [57, Definition 10]) define uniqueness unconditionally: that is, for a validly generated public key, each

[11] The birthday paradox does not apply here, so that for a 128-bit security level is suffices to have c be 128 bits long.

input α to the VRF has at most one hash output β that can be proven to be correct. However, the construction in Section 3.5 satisfies it only computationally: more than one hash output y may exist, but only one valid β—the one produced by $F_{SK}(\alpha)$—can be proven correct by any computationally bounded adversary, even given the secret key. We are not aware of any prior work defining this relaxation of the uniqueness property, although Chase and Lysyanskaya [27] mention that such a relaxation can be defined. We therefore define it here. Our definition is in terms of concrete, rather than asymptotic security, because concrete security enables us to set length parameters.

DEFINITION B.1. *(Computational Trusted Uniqueness.) A VRF satisfies (Q_H, ϵ)-trusted uniqueness if for all adversaries A that makes at most Q_H queries to the random oracle, for a validly chosen key pair (PK, SK),*

$$\begin{aligned}\Pr[&A(PK, SK) \to (\alpha, \beta_1, \pi_1) \text{ and} \\ &(F_{SK}(\alpha), \Pi_{SK}(\alpha)) \to (\beta_2, \pi_2) \text{ s.t.} \\ &\beta_1 \neq \beta_2 \text{ and } \mathsf{Ver}_{PK}(\alpha, \beta_1, \pi_1) = 1] \leq \epsilon\,.\end{aligned}$$

(Naor and Ziv [57, Definition 10]) also require that for every PK, for an overwhelming fraction of the domain of α, there exists β and π such that $\mathsf{Ver}_{PK}(\alpha, \beta, \pi) = 1$; we retain this requirement, which is trivially satisfied by our VRF, because Π and F work for every α.)

We now prove that the VRF satisfies Definition B.1 unconditionally (based on the randomness of the oracle H_3 and not on any computational assumptions).

CLAIM B.2. *The VRF satisfies (t, ϵ)-computational trusted uniqueness of Definition B.1 for $\epsilon = (Q_H + 1)/\min(q/2, \rho)$, where $\rho = |\text{range}(H_3)|$ and $Q_H \leq t$ is the number of queries the adversary makes to the random oracle H_3.*

Note that the quantitative bound on ϵ in the above claim implies that the bit length $\log \rho$ of the output c of H_3 can be equal to the desired security level; in particular, it can be shorter than q (*i.e.,* the prime order of the cyclic group G). This claim is the only part of the security analysis affected by the output length of H_3.

PROOF. Suppose there is an adversary A that violates computational trusted uniqueness with probability ϵ. That is, on input g, x, the adversary A makes Q_H queries to the H_3 oracle and wins by outputting (α, β_1, π_1) s.t. $\beta_1 \neq \beta_2$ and $\mathsf{Ver}(\alpha, \beta_1, \pi_1) = 1$ with probability ϵ. We will show that $\epsilon \leq (Q_H + 1)/\min(q/2, \rho)$, where q is the order of the group G and $\rho = |\text{range}(H_3)|$.

The proof π_1 contains γ_1 such that $\beta_1 = H_2(\gamma_1)$; similarly, π_2 contains γ_2 such that $\beta_2 = H_2(\gamma_2)$. Since $\beta_1 \neq \beta_2$, we have $\gamma_1 \neq \gamma_2$. Therefore, since $\gamma_2 = [H_1(\alpha)]^x$ (because that is what Π produces), we have $\gamma_1 \neq [H_1(\alpha)]^x = h^x$.

Now, it must be that $\pi_1 = (\gamma_1, c, s)$ for some c, s that ensure that $\mathsf{Ver}(\alpha, \beta_1, \pi_1) = 1$. The verification function Ver computes $h = H_1(\alpha)$ and

$$\begin{aligned}u &= g^s (g^x)^c \\ v &= h^s (\gamma_1)^c.\end{aligned}$$

Note that $h \neq 1$ (since H_1 maps to $G - \{1\}$), and thus, because G is of prime order, h is a generator of G. Then we can take the logarithm of the first equation base g and the logarithm of the second equation base h, because h and g are generators of G, and the verification procedure checks that $\gamma_1 \in G$. Solving these for s we get

$$\begin{aligned}\log_g u - cx &\equiv s \pmod q \\ \log_h v - c \log_h \gamma_1 &\equiv s \pmod q\end{aligned}$$

which implies that

$$c \equiv \frac{\log_g u - \log_h v}{x - \log_h \gamma_1} \pmod q \tag{4}$$

Since $\gamma_1 \neq h^x$, the denominator is not zero, and so there is only one c modulo q that satisfies equation (4) given g, g^x, h, γ_1, u, and v.

Recall that for verification to pass,

$$c = H_3(g, h, g^x, \gamma_1, u, v)\,.$$

Note that the contents of the query to H_3 contains every value in the right hand side of the equations (4), and thus the correct c is uniquely defined at the time the query is made.

What is the probability, for a given query to H_3, that the random value returned by the H_3 oracle is congruent to that correct c modulo q? Let ρ denote $|\text{range}(H_3)|$. If the range of H_3 is a subset of Z_q, and the correct c is in that range, then this probability is at most $1/\rho$. If ρ is an exact multiple of q, then this probability is at most $1/q$. Finally, if ρ not an exact multiple of q but is greater than q, then some values modulo q are more likely than others, but none will have probability greater than $\lceil \rho/q \rceil / \rho < 2/q$.

Assume the adversary outputs β_1, π_1 and then the verification algorithm is run. This causes a total of $Q_H + 1$ queries to H_3 (Q_H by A and one by the verifier), so by the union bound, the chances that any of them returns a correct c for that query are at most $(Q_H + 1)/\min(q/2, \rho)$. □

Remark. Since our computational trusted uniqueness property is slightly weaker than the unconditional trusted uniqueness of [57, Definition 10], the proof of the soundness property in [57, Theorem 4] of Naor-Ziv needs a slight change, as follows. Recall that the

proof is a reduction from an adversary A who violates soundness to an adversary B who forges signatures. The reduction relies on the fact that A must provide the correct β value (called y in [57]) and proof π for the VRF as part of its soundness-violating output on an input α (called x in [57]). Computational trusted soundness ensure that this happens except with negligible (i.e., $(Q_H+1)/\min(q/2,\rho)$) probability. Thus, the success probability of the reduction reduces from ϵ to $\epsilon-(Q_H+1)/\min(q/2,\rho)$.

Uniqueness Without Trusting the Key Our VRF can be modified to attain the stronger property of computational uniqueness (without needing to trust the key generation). The verifier simply needs to check that the group G is really of prime order q and that g and the public key are in $G-\{1\}$. These properties suffice for the proof above to go through regardless of how key generation was performed.

B.2.2 Pseudorandomness.

We will state and prove pseudorandomness in terms of concrete, rather than asymptotic, security. This type of security is more relevant to practice and works for a fixed group G.

We require a slight modification to the notions of pseudorandomness and selective pseudorandomness from [57, Definition 11]: instead of being indistinguishable from a random bit string, the output of our VRF is indistinguishable from a truncation of a random element of $G-\{1\}$, i.e., from the distribution $H_2(U_G)$, where U_G is the uniform distribution on $G-\{1\}$. Our definitions are thus as follows.

Definition B.3. *(Pseudorandomness) A VRF satisfies (t,Q_H,Q_P,ϵ) pseudorandomness for output distribution S if no adversary D whose running time and description size are bounded by t, whose total number of random oracle queries is bounded by Q_H and total number of Π and F queries is bounded by Q_P, can distinguish the following two games with advantage more than ϵ. In the both games, VRF keys (PK,SK) are honestly generated, and $D(PK)$ gets to query Π_{SK}, F_{SK}, and the random oracles on arbitrary inputs. In both games, D chooses a challenge input α^* that has been queried to neither Π nor F. In one game, D receives $F_{SK}(\alpha^*)$, while in the other D receives a random element drawn from S. Finally, after additional queries to Π_{SK} and F_{SK} (except on α^*), D outputs one bit indicating which game D thinks it is playing.*

The slightly weaker notion of selective *pseudorandomness is defined the same way, except D has to choose α^* before any queries and before seeing PK.*

Pseudorandomness of our VRF depends on the following assumption about the group G and generator g, known as the (t,ϵ)-*DDH (Decisional Diffie-Hellman) Assumption*: for any adversary C whose description size and running time are bounded by t, the difference in probabilities (where the probabilities are over a random choice of $g,h,h'\in G-\{1\}$ and $x\in\{1,\ldots,q\}$) that $C(g,g^x,h,h^x)=1$ and $C(g,g^x,h,h')=1$ is at most ϵ.

We now prove that our VRF satisfies both pseudorandomness and selective pseudorandomness. We address selective pseudorandomness first, because it is simpler.

Claim B.4. *Under the (t,ϵ)-DDH assumption, for any Q_H,Q_P, the VRF satisfies (t',Q_H,Q_P,ϵ') selective pseudorandomness for output distribution $H_2(U_G)$, for $t'\approx t$ (minus the time for $\Theta(Q_H+Q_P)$ exponentiations in G and one evaluation of H_2) and $\epsilon'=\epsilon+Q_P(Q_P+Q_H)/q$.*

Proof. We need to show the following: if

- D chooses α^*,
- then receives an honestly generated $PK=g^x$ and
  - either $H_2([H_1(\alpha^*)]^x)$
  - or H_2 applied to a random element of G,
- is allowed Q_H queries to random functions H_1 and H_3 and Q_P queries are to Π_{SK} or F_{SK} (except on α^*)
- can distinguish between the two cases with advantage ϵ'

then we can build C that breaks (t,ϵ)-DDH assumption for $t\approx t'$ (plus the time for $\Theta(Q_H+Q_P)$ exponentiations in G and one evaluation of H_2) and $\epsilon=\epsilon'-Q_P(Q_P+Q_H)/q$.

Because F_{SK} is computable, in our case, from Π_{SK}, we can assume without loss of generality that D never queries F_{SK}—every query to F_{SK} can be replaced with a query to Π_{SK}.

Given (g,g^x,h,h') (where h' is either h^x or a random element of $G-\{1\}$), C gets α^* from D, sets (g,g^x) as the VRF public key PK and runs $D(PK,H_2(h'))$, answering the queries of D as follows (note that all random oracle query responses are computed as below unless already defined):

- If D queries α^* to random oracle H_1, C returns h.
- If D queries any other α_i to H_1, C chooses a random $\rho_i\in\{1,\ldots,q\}$ and then programs H_1 as
$$H_1(\alpha_i):=g^{\rho_i}.$$
(note that this response is distributed uniformly in $G-\{1\}$, just a like the honest H_1, because g is a generator of G).
- If D queries H_3, C return a fresh random value in the appropriate range (note that these responses are distributed just like honest H_3).
- If D makes a query q_i to Π (note that $q_i\neq\alpha$),
  - C makes a query to $H_1(q_i)$ as described above to get ρ_i,
  - C sets $\gamma=(g^x)^{\rho_i}$,

– C chooses random values $s \in [q]$ and $c \in \text{range}(H_3)$ and then computes

$$u = g^s (g^x)^c$$

and

$$v = [g^{\rho_i}]^s [(g^x)^{\rho_i}]^c .$$

(Note that $u, v, x, h = g^{\rho_i}, s$, and c are distributed identically to the distribution produced by Π: the difference in how these distributions are obtained is simply that Π chooses a uniform k while C chooses a uniform s, where k and s are tied by the equation $s + cx \equiv k \pmod q$, and $u = g^k$, $v = h^k$.) If $H_3(g, g^{\rho_i}, g^x, (g^x)^{\rho_i}, u, v)$ is already defined, then C fails and aborts. Else, C programs the H_3 oracle to let

$$H_3(g, g^{\rho_i}, g^x, (g^x)^{\rho_i}, u, v) := c$$

(note that if C does not abort, then H_3 is uniformly random, just like honest H_2 and H_3).

If C does not abort, then its simulation for D is faithful and C can just output what D outputs. The probability that C aborts is simply the probability that $H_3(g, g^{\rho_i}, g^x, (g^x)^{\rho_i}, u, v)$ is already defined during the computation of the response to Π; since at most $Q_H + Q_P$ values of H_3 are defined, and u is a uniformly random value in G (because s is uniformly random in $[q]$ and g is a generator), the chances that a single query to Π causes an abort are $(Q_H + Q_P)/q$, and the chances that any of the queries to Π causes an abort are $Q_P(Q_H + Q_P)/q$. Thus, the advantage of C is at least $\epsilon' - Q_P(Q_P + Q_H)/q$. □

We can also prove pseudorandomness, but with a looser security reduction than selective pseudorandomness.

Claim B.5. *Under the (t, ϵ)-DDH assumption, for any $Q_H \geq 1, Q_P$, the VRF satisfies $(t', Q_H, Q_P, \epsilon')$ pseudorandomness for output distribution $H_2(U_G)$, for $t' \approx t$ (minus the time for $\Theta(Q_H + Q_P)$ exponentiations in G and one evaluation of H_2) and $\epsilon' = 4\epsilon Q_P + Q_P(Q_P + Q_H)/q$.*

Proof. We explain the proof by showing the differences from the previous proof. The problem is that C does not know what α^* is—it could be in any of the H_1 queries. We follow the approach of [29] to deal with this problem.

Whenever D makes a query α_i to H_1, C flips a biased coin to decide whether this query is going to be "type-sig" (with probability $Q_P/(Q_P + 1)$) or "type-attack" (with probability $1/(Q_P+1)$). If the query is "type-sig," then C works the same way as in the proof of Claim B.4. Else, C returns h^{ρ_i} for a random $\rho_i \in \{1, \ldots, q\}$. C remembers the type of the query and the ρ_i value.

If D makes a query q_i to Π, then C aborts if $q_i = \alpha_i$ for an α_i of type-attack (else C proceeds as before). At some point D produces α^*; before proceeding, C makes sure α^* has been queried to H_1 (performing the query if it hasn't been). C aborts if $\alpha^* = \alpha_i$ for some α_i of type-sig, and otherwise returns $H_2(h'^{\rho_i})$ as the response to the challenge.

We note that all the responses to H_1 queries are still uniformly distributed over $G - \{1\}$ and independent, because both g and h are generators of G. if $h' = h^x$, then D receives the correct value for $F_{SK}(\alpha^*)$, namely $H_2(h'^{\rho_i}) = H_2(h^{x\rho_i}) = H_2([H_1(\alpha^*)]^x)$. On the other hand, if h' is a uniform element of $G - \{1\}$, then instead of instead of $F_{SK}(\alpha^*)$, D receives a uniform response chosen independently of anything else from from $H_2(G - \{1\})$ because a uniform value raised to a fixed nonzero power is uniform in $G - \{1\}$.

Now C succeeds as long as the guesses for the H_1 query type (type-sig or type-attack) don't lead to an abort (and also an abort due to a collision of H_3 inputs doesn't happen, as in the proof of Claim B.4). Note that these guesses are independent of the view of D and therefore of the success of D. The probability that the guesses are correct for each Π query and for α^* is

$$\left(\frac{Q_P}{Q_P + 1}\right)^{Q_P} \frac{1}{Q_P + 1} \geq \frac{1}{4Q_P}$$

whenever $Q_P \geq 1$ (as can be seen by observing that the left-hand multiplied by Q_P is increasing, and its value at $Q_P = 1$ is $1/4$). We thus obtain the claimed result. □

B.2.3 Collision Resistance

We now define trusted collision resistance, which states that an adversary cannot produce a collision even given SK, as long as the keys are honestly generated. This property, while not explicitly defined in [57], is necessary to ensure the completeness of NSEC5, i.e., to ensure that a valid non-existence proof can always be generated by the nameserver and accepted by the resolver whenever the record does not exist (see [57, Proof of Theorem 4]).

Definition B.6. *(Trusted Collision Resistance) A VRF satisfies (Q_H, ϵ) trusted collision resistance if no adversary making Q_H random oracle queries, can, given an honestly generated SK, output two values $\alpha_1 \neq \alpha_2$ such that $F_{SK}(\alpha_1) = F_{SK}(\alpha_2)$ with probability greater than ϵ.*

Claim B.7. *If every output of H_2 has at most τ preimages in G, then our VRF satisfies $(Q_H, \tau Q_H^2/(2q))$-trusted collision resistance. Note that in our suggested instantiation of H_2, $\tau = 2$, so we have $(Q_H, Q_H^2/q)$-trusted collision resistance*

PROOF. The argument is simple: Q_H attempts produce Q_H uniformly random (because H_1 is a random oracle and raising to the power x is a permutation) values $\gamma \in G - \{1\}$; the probability that any pair of them collide after the application of H_2 is at most $\tau/(q-1)$, and there are $(Q_H-1)(Q_H)/2$ pairs, for a total collision probability (by the union bound) of $2^\tau Q_H(Q_H-1)/(2(q-1))$, which is less than $2^\tau Q_H^2/(2q)$ whenever $Q_H < q$. □

Collision Resistance Without Trusting the Key Similarly to the case with uniqueness, our VRF can be modified the same way to attain collision resistance without needing to trust the key generation.

C. SECURITY OF THE RSA-BASED VRF

In [40] the authors provided an explicit proof only for the selective pseudorandomness of the RSA-based construction [40, Lemma III.2], but neither for its trusted uniqueness nor for its collision resistance. While these proofs are straightforward, we provide them here for completeness.

CLAIM C.1. *The RSA-based VRF of [40] satisfies trusted uniqueness as per [57, Definition 10]).*

PROOF. The claim that for every α there exist β, π such that $\mathsf{Ver}_{PK}(\alpha, \beta, \pi) = 1$ follows by inspection since for every α it is true that $\mathsf{Ver}_{PK}(\alpha, \mathit{Prove}_{SK}(\alpha)) = 1$.

Let A be an adversary such that $A(PK, SK) \to (\alpha, \beta_1, \pi_1)$ and $\mathit{Prove}_{SK}(\alpha) \to (\beta_2, \pi_2)$ and $\beta_1 \neq \beta_2$, where $(PK, SK) \leftarrow \mathit{Setup}(1^\kappa)$. Since $\beta_1 \neq \beta_2$ it follows that $\pi_1 \neq \pi_2$ as $\beta_i = H(\pi_i)$ for $i = 1, 2$ and $H(\cdot)$ implements a deterministic function. For the same reason, the value of $MGF(\alpha)$ is fully determined by α. Since PK, SK are valid RSA keys, the function $f(x) = x^e$ is a bijection in $\mathbb{Z}_N$ (where e is the RSA public exponent) and therefore $\pi_1^e \neq MGF(\alpha) = \pi_2^e$. Due to this, the probability that Ver_{PK} will accept for proof π_1 and value β_1 for input α is 0. □

CLAIM C.2. *The RSA-based VRF of [40] for H with output size ℓ (assuming ℓ is less than the length of the RSA modulus) satisfies $(Q_H, Q_H^2/2^{\ell+1})$-trusted collision resistance per definition B.6.*

PROOF. Indeed, for a collision to occur, either $H(\pi_1)$ should equal $H(\pi_2)$ for some $\pi_1 \neq \pi_2$, or $MGF(\alpha_1)$ should equal $MGF(\alpha_2)$ for $\alpha_1 \neq \alpha_2$. (Because trusted key generation ensures that raising to the power d is a permutation.) Let Q'_H be the number of queries to H and Q''_H be the number of queries to MGF. Let k be the output size of the MGF. The probability of collision, by the union bound, is at most $Q_H'^2/(2\cdot 2^\ell) + Q_H''^2/(2\cdot 2^k) \leq Q_H^2/2^{\ell+1}$ because $k \leq \ell$. □