

dnsop@IETF'98
Chicago, March 2017

draft-vcelak-nsec5-04

NSEC5: DNSSEC Authenticated Denial of Existence

Jan Vcelak (CZ.NIC)

Sharon Goldberg (Boston University)

**Dimitrios Papadopoulos (University of
Maryland)**

Shumon Huque (Salesforce)

**YO DAWG, I HERD YOU LIKE
VERIFYING**

**SO I PUT A SIGNATURE IN YOUR HASH
SO YOU CAN VERIFY WHILE YOU VERIFY**

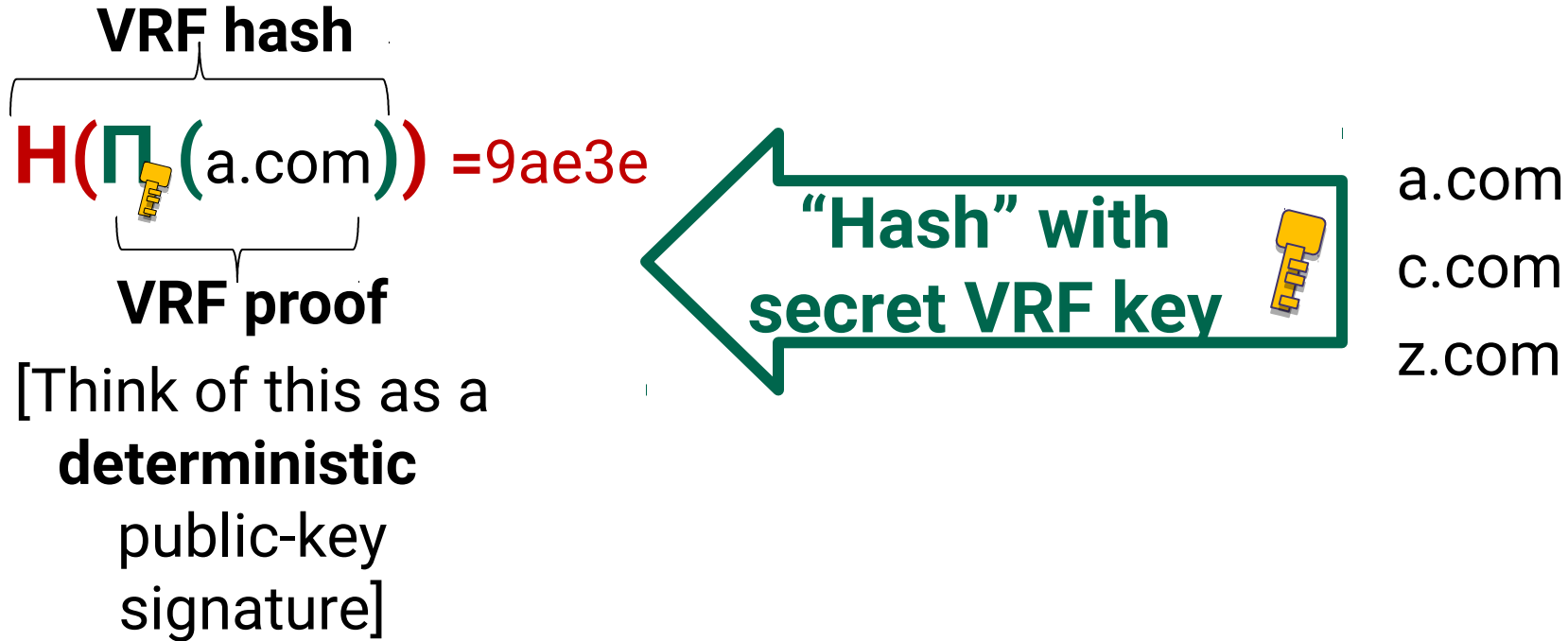
memegenerator.net

DNSSEC Authenticated Denial of Existence

	No offline zone enumeration	Integrity vs outsiders	Integrity vs compromised nameserver	No online crypto
DNS (legacy)	✓	✗	✗	✓
NSEC or NSEC3	✗	✓	✓	✓
Online Signing ("NSEC3 White	✓	✓	✗	✗
NSEC5	✓	✓	✓	✗

NSEC5 replaces **SHA1** used in NSEC3 with a **Verifiable Random Function (VRF)** [draft-goldbe-vrf-00] that resolvers cannot compute offline.

offline signing with **NSEC5**



- * **NSEC5-ECC**: VRF based on elliptic curves
 - **[draft-goldbe-vrf-00]**. (Presented at SAAG, Thursday!)
 - Has a formal cryptographic security proof.
 - For 256-bit elliptic curves, π gives 641-bit outputs.

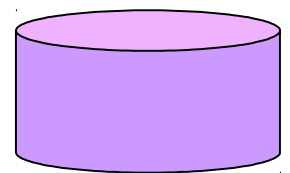
answering queries with NSEC5

PROOF
aa8678

Π (q.com)
 $H(aa867) = 7a89b$

Public Zone Signing Key (ZSK)

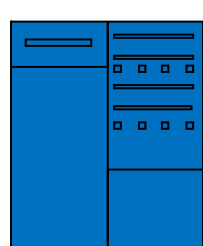
Public VRF Key



q.com?

PROOF
aa8678

NSEC5
3cd91.com
8cb67.com



a.com
c.com
z.com

secret VRF key

NSEC5
3cd91.com

NSEC5
8cb67.com

NSEC5
8cb67.com

NSEC5
9ae3e.com

NSEC5
9ae3e.com

NSEC5
3cd91.com

To verify:

Does NSEC5 cover PROOF?

$$3cd19 < H(aa8678) < 8cb67$$

Does PROOF match query?

VER (q.com, aa8678)

[Think of this as a signature verification]

DNSSEC Authenticated Denial of Existence

	No offline zone enumeration	Integrity vs outsiders	Integrity vs compromised nameserver	No online crypto
DNS (legacy)	✓	✗	✗	✓
NSEC or NSEC3	✗	✓	✓	✓
Online Signing ("NSEC3 White Lies")	✓	✓	✗	✗
NSEC5	✓	✓	✓	✗

Because resolvers cannot compute VRF hashes offline

In **[NDSS'15]** we proved this is **necessary** to prevent zone enumeration & have integrity

Because the nameserver doesn't know the zone-signing key

NSEC5 spec & implementation



Knot DNS

authoritative nameserver



Unbound

recursive resolver

&

-04 draft includes DNS-level optimizations:

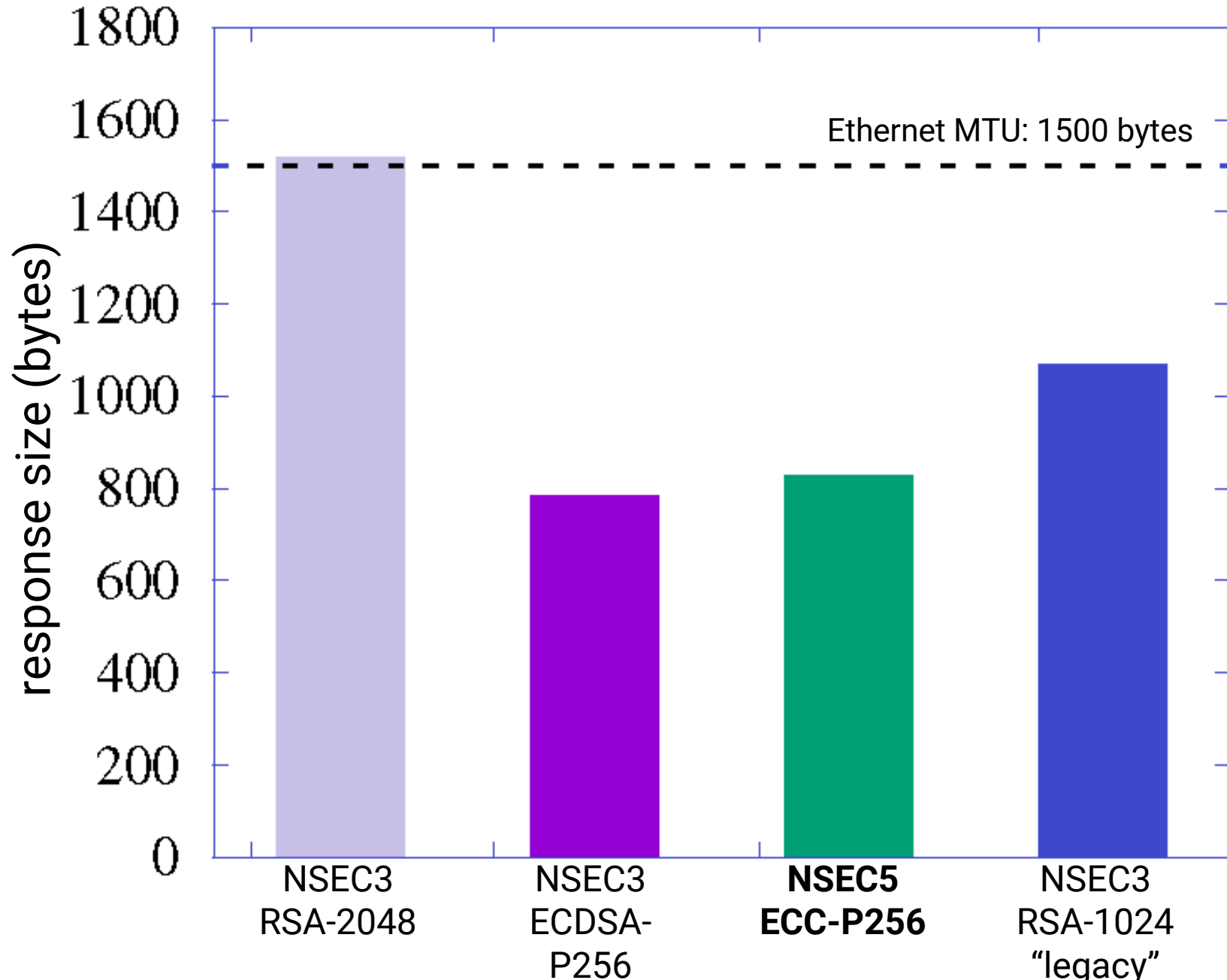
1. The wildcard bit from **[draft-gieben-nsec4-00]**
2. Precomputed closest encloser proofs mentioned in **[RFC7128]**

9K Lines of Code, no new libraries (openssl) or system optimizations

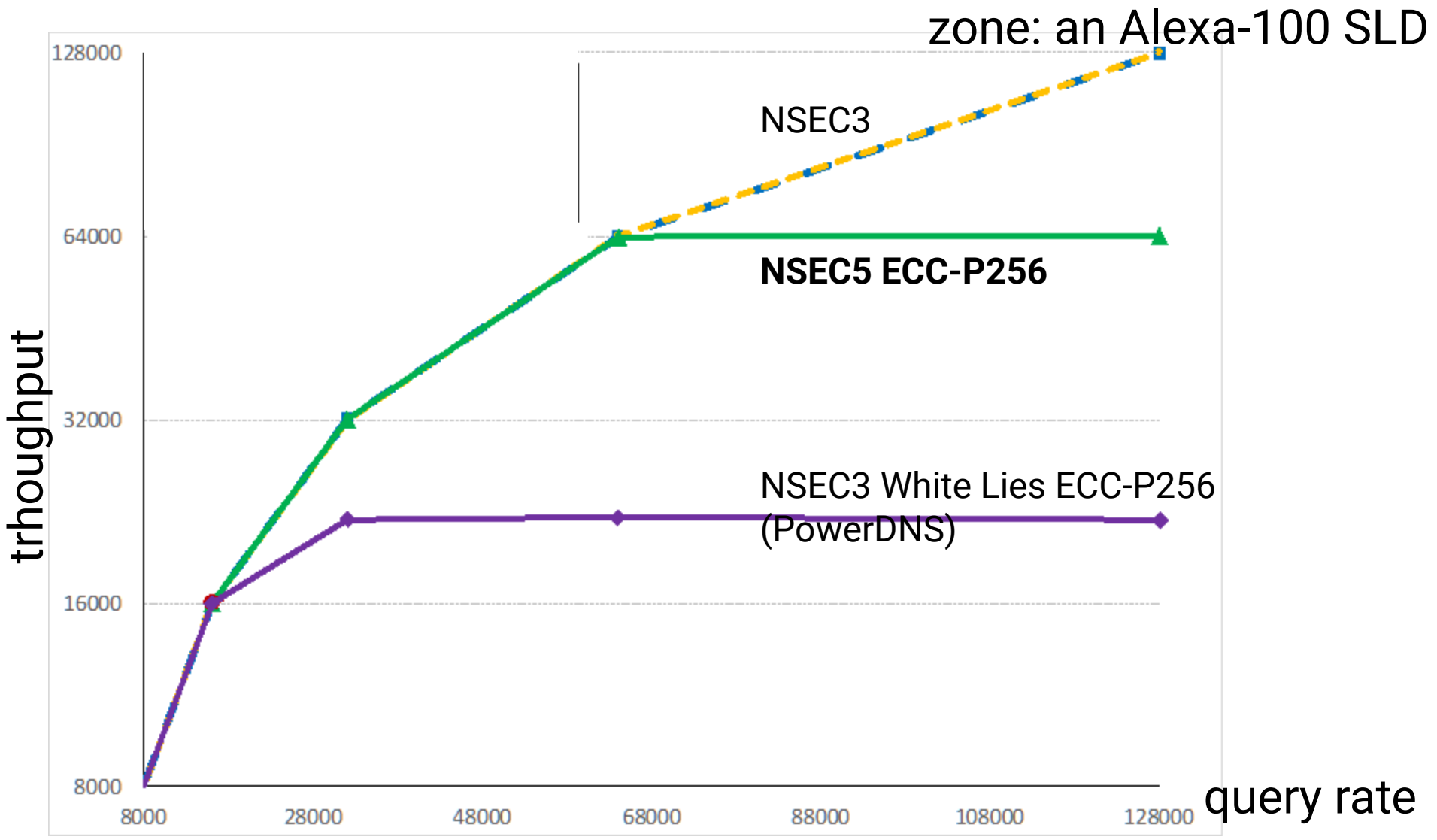
Current implementations support P-256 curve.

Could be faster with Ed25519 curve included in the -04 draft

empirical measurement of NXDOMAIN response sizes



nameserver query throughput (steady rate, NXDOMAIN)



Machine specs: 20X Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz Dual Mode (Total 24 threads on 40 virtual CPUs) 256GB RAM running CentOS Linux 7.1

questions?

- Research paper with performance numbers & crypto proofs:
<http://ia.cr/2017/099>
- NSEC5 Project page_
<https://www.cs.bu.edu/~goldbe/papers/nsec5.html>
- Long preso on NSEC5 at Real World Crypto (RWC'17)
<https://www.youtube.com/watch?v=-pWrij0YhGo>

dnsreactions...



Hearing about NSEC5



When I finally grasp NSEC5

backup slides

offline zone signing with NSEC3 [RFC5155]

SHA1(a.com) = a1bb5

SHA1(c.com) = 23ced

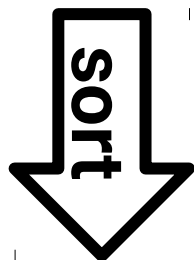
SHA1(z.com) = dde45

a.com

c.com

z.com

Hash names



23ce
d

a1bb
5

dde4
5

Sign NSEC3 records
with secret ZSK

NSEC3 23ced.com
a1bb5.com
NSEC3 a1bb5.com
NSEC3 dde45.com

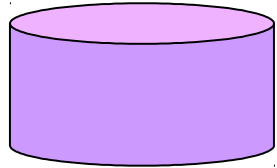
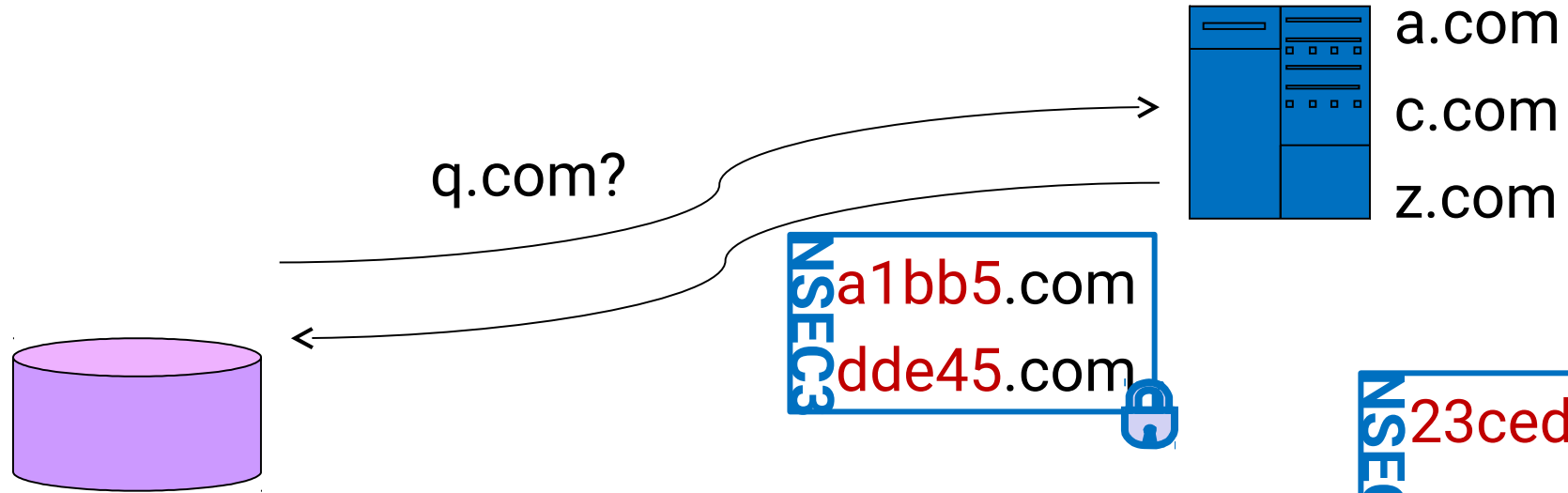
NSEC3 dde45.com
NSEC3 23ced.com



answering queries with NSEC3

Public Zone Signing Key (ZSK) 

SHA1(q.com) = c987b



Step 1: Collect

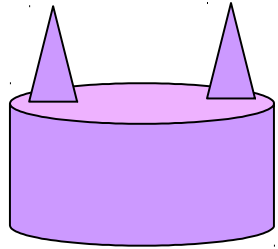
a1bb5.com
dde45.com



offline zone enumeration with NSEC3

Public Zone Signing Key (ZSK) 


SHA1(r.com) = 33c46



r.com?



a.com
c.com
z.com

NSEC3
23ced.com
a1bb5.com 

Step 1: Collect



a1bb5.com
dde45.com

Offline dictionary attack

Step 2: Crack

a.com
z.com
c.com

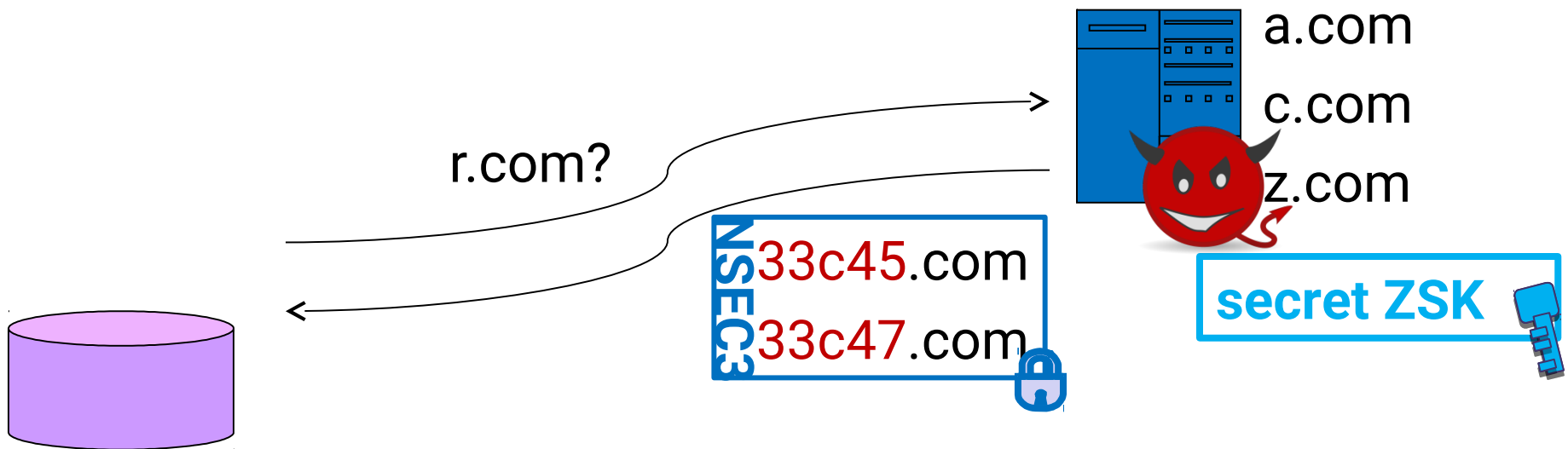
NSEC3
23ced.com 
a1bb5.com 
NSEC3
a1bb5.com 
NSEC3
dde45.com 

NSEC3
dde45.com 
NSEC3
23ced.com 

online signing stops zone enumeration!

Public Zone Signing Key (ZSK) 

SHA1(r.com) = 33c46



“NSEC3 White Lies” [RFC7128]