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)
David C. Lawrence (Akamai)

DNSSEC Authenticated Denial of Existence

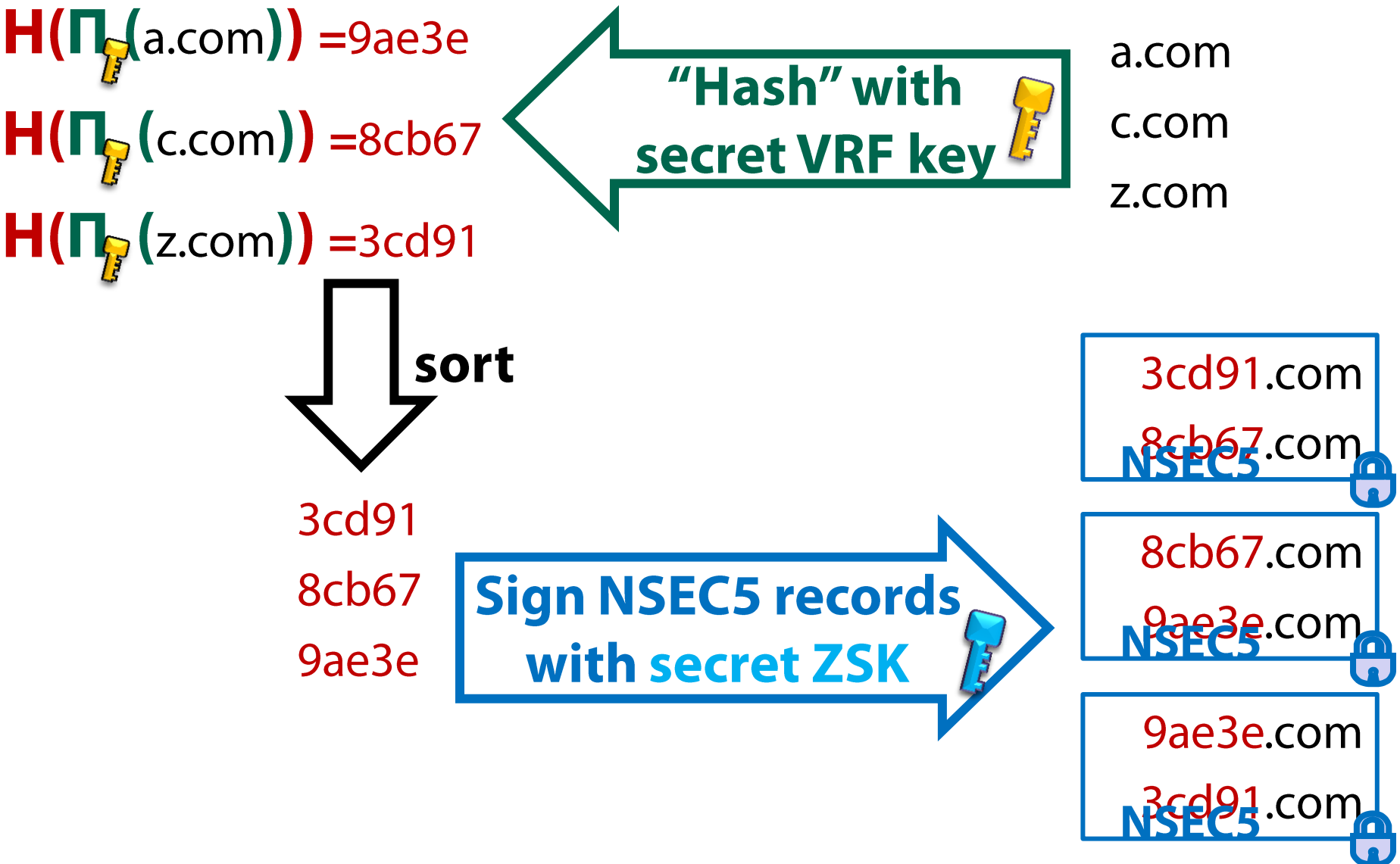
	No offline zone enumeration	Integrity vs outsiders	Integrity vs compromised nameserver	No online crypto
DNS (legacy)	✔	X	X	✔
NSEC or NSEC3	X	✔	✔	✔
Online Signing ("NSEC3 White Lies")	✔	✔	X	X
NSEC5	✔	✔	✔	X

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

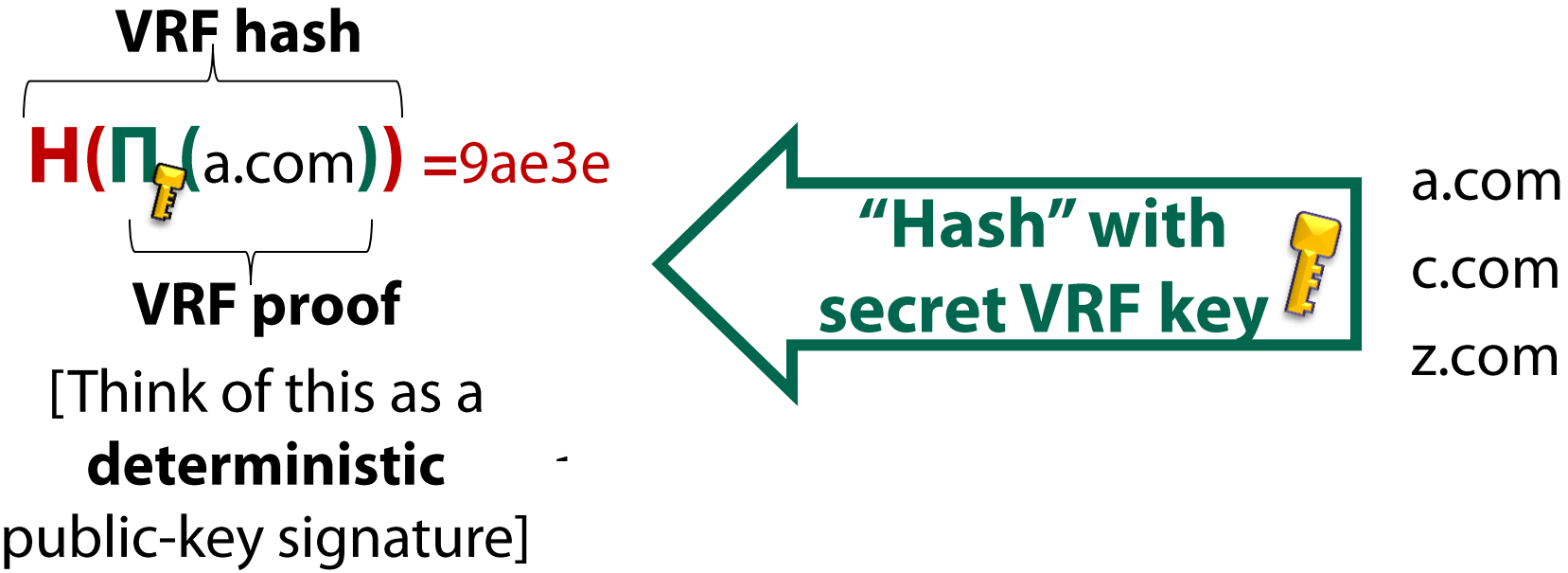
offline signing with NSEC5

offline signing with NSEC5

offline signing with NSEC5

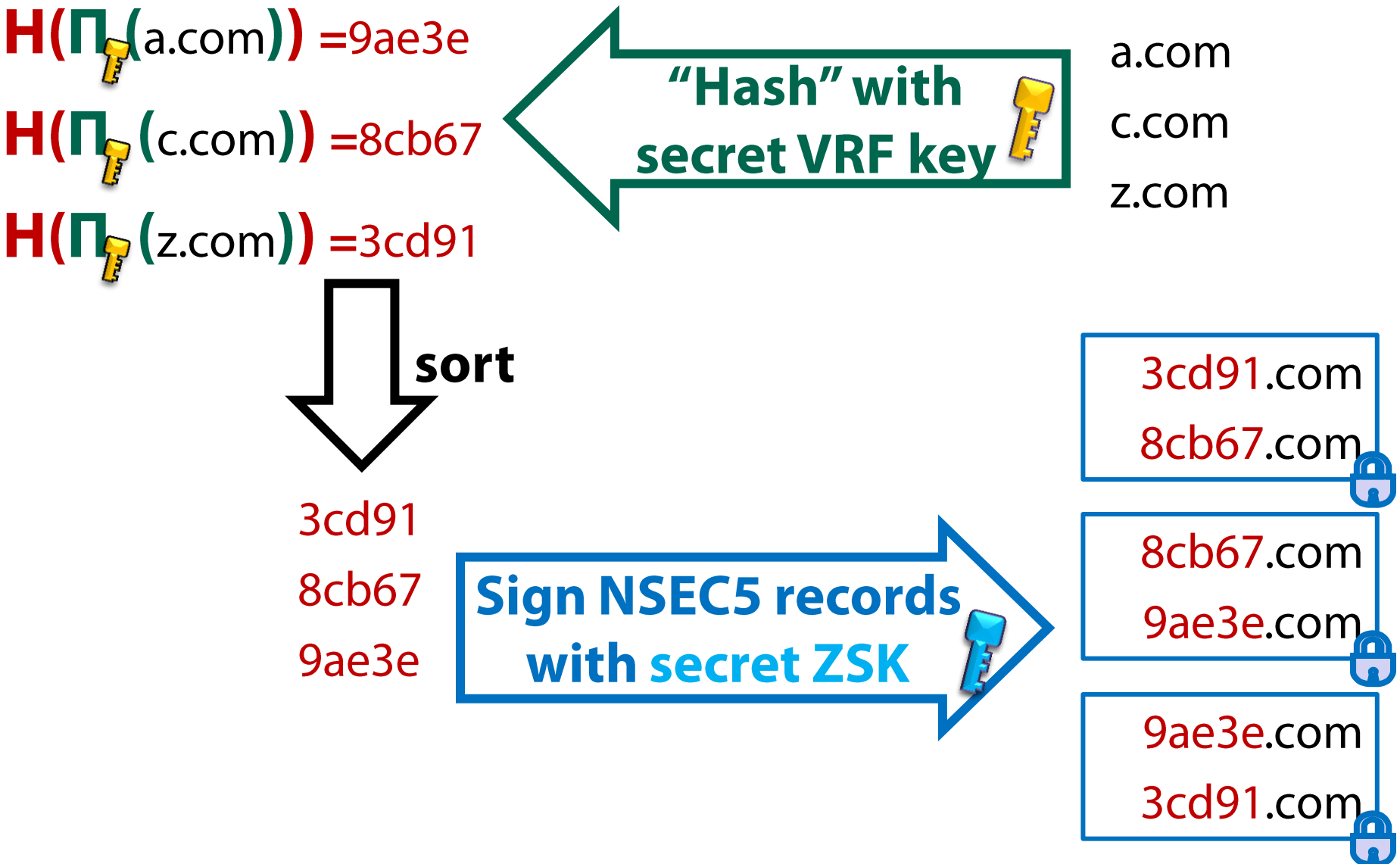


offline signing with NSEC5



* **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.

offline signing with NSEC5

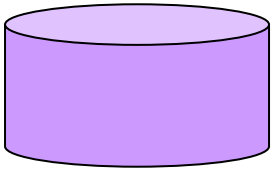


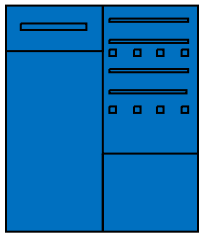
answering queries with NSEC5

Public Zone Signing Key (ZSK):

Public VRF Key:

q.com?





a.com

c.com

z.com

Π_{key}(q.com)=aa8678

H(aa867)=7a89b

secret VRF key

3cd91.com

8cb67.com

8cb67.com

9ae3e.com

9ae3e.com

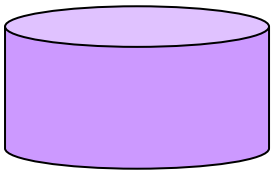
3cd91.com

answering queries with NSEC5

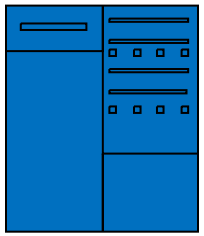
Public Zone Signing Key (ZSK):

Public VRF Key:

q.com?



3cd91.com
8cb67.com



a.com
c.com
z.com

$\Pi_{}$(q.com)=

PROOF
aa8678

H(aa867)=7a89b

secret VRF key

3cd91.com
8cb67.com

8cb67.com
9ae3e.com

9ae3e.com
3cd91.com

answering queries with NSEC5

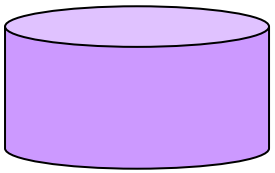
Public Zone Signing Key (ZSK):

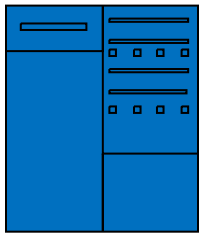
Public VRF Key:

Π(q.com)=aa8678

H(aa867)=7a89b

q.com?





a.com

c.com

z.com

PROOF
aa8678

3cd91.com

8cb67.com

secret VRF key

3cd91.com

8cb67.com

8cb67.com

9ae3e.com

9ae3e.com

3cd91.com

answering queries with NSEC5

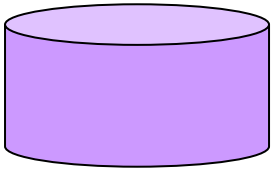
Public Zone Signing Key (ZSK):

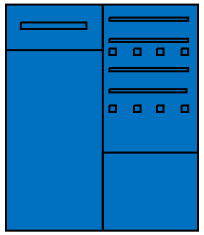
Public VRF Key:

$\Pi_{}$(q.com)=aa8678

H(aa867)=7a89b

q.com?





a.com

c.com

z.com

PROOF
aa8678

3cd91.com

8cb67.com

secret VRF key

3cd91.com

8cb67.com

8cb67.com

9ae3e.com

9ae3e.com

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)	✔	X	X	✔
NSEC or NSEC3	X	✔	✔	✔
Online Signing ("NSEC3 White Lies")	✔	✔	X	X
NSEC5	✔	✔	✔	X

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

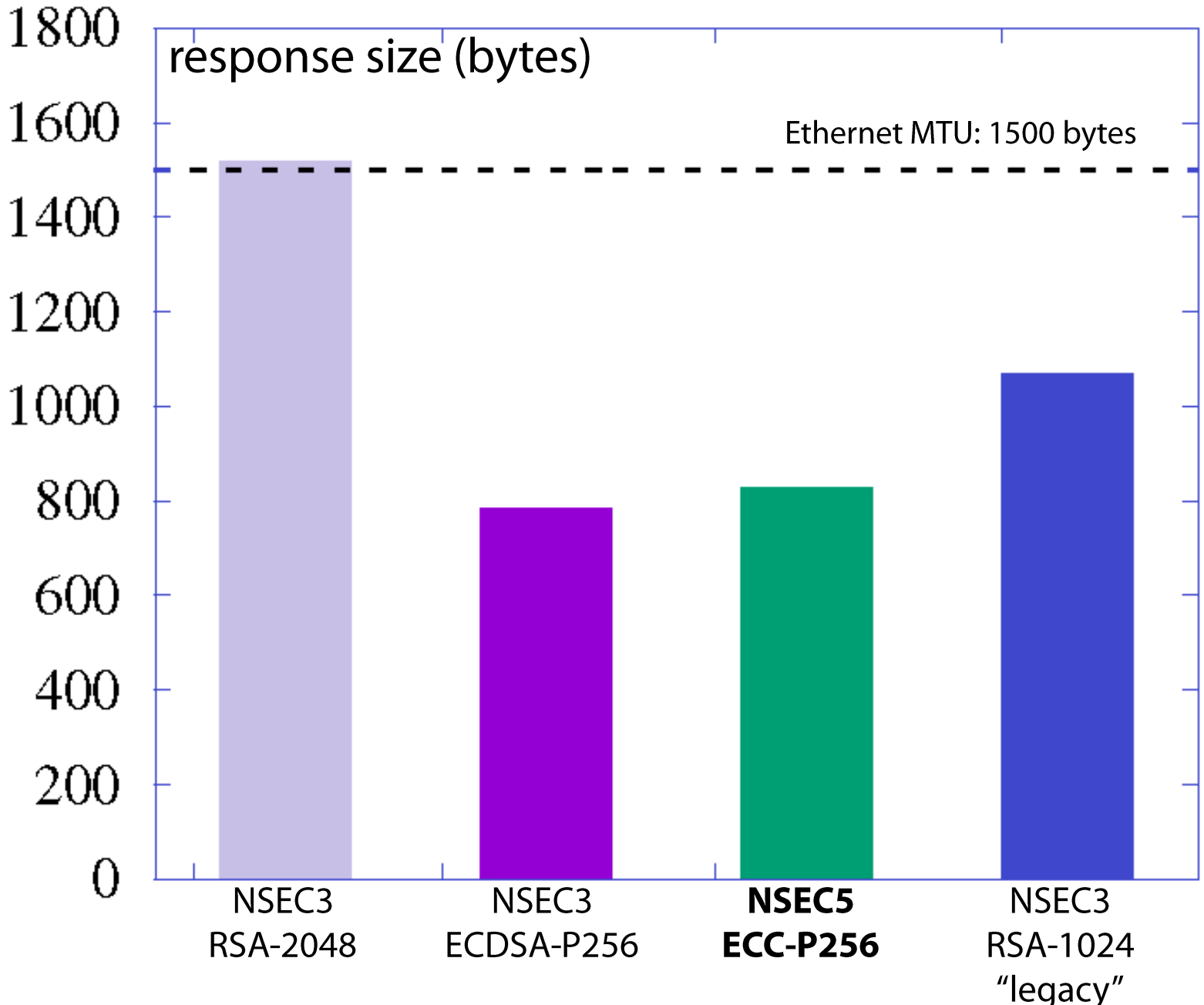
-04 draft includes DNS-level optimizations:

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

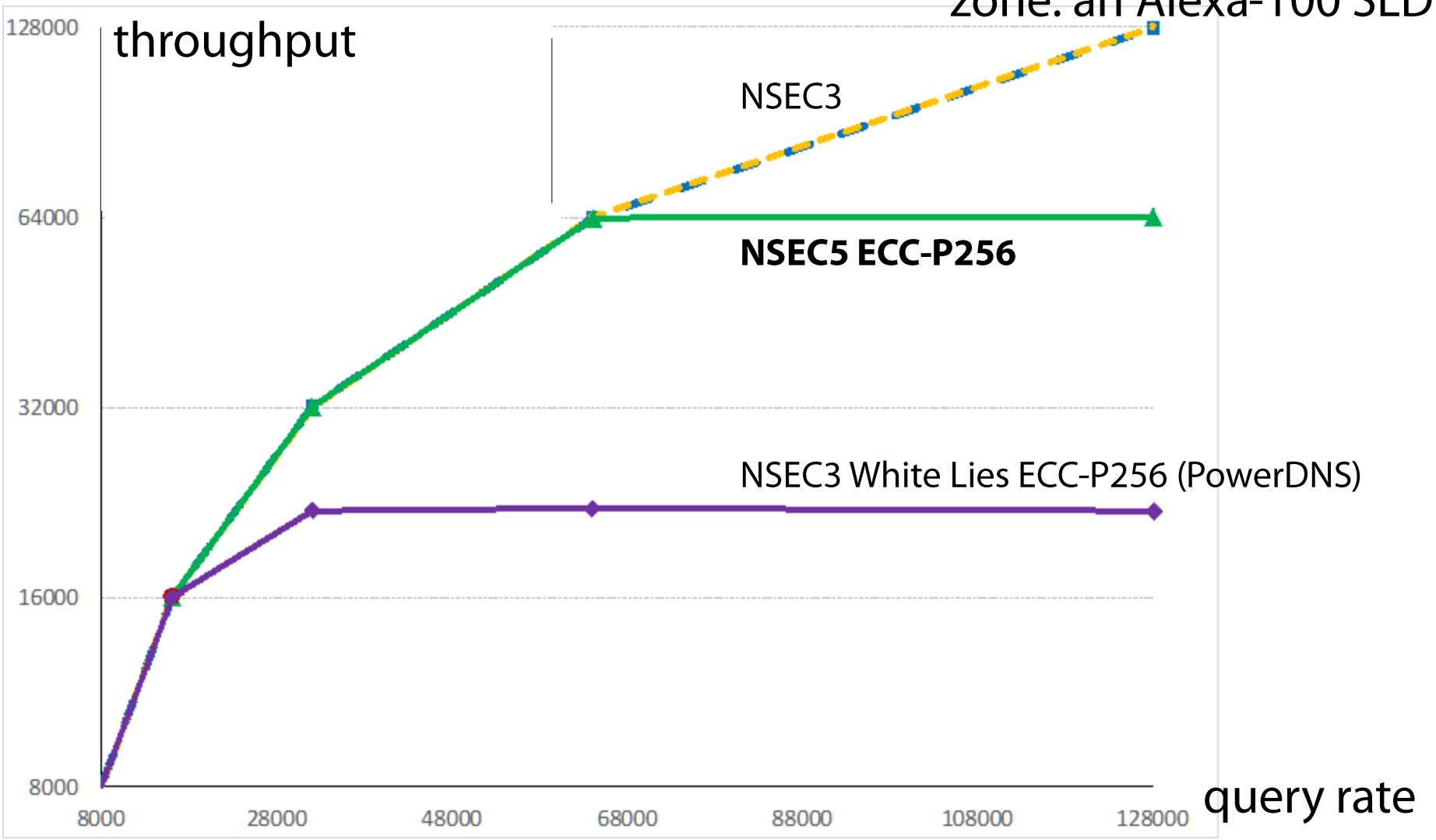
9K Lines of Code, no new libraries (openSSL) or system optimizations

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

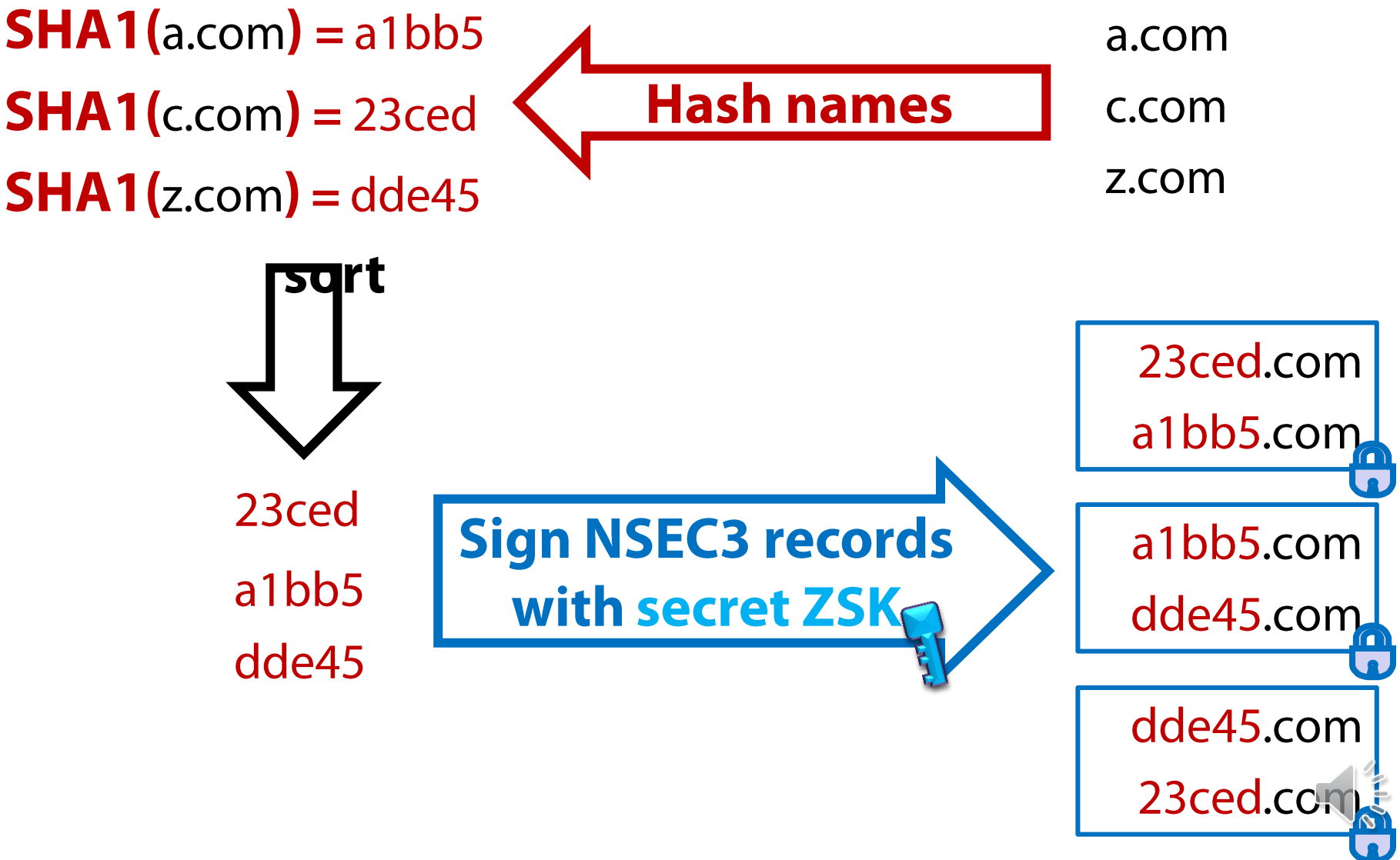
dnsreactions…

Hearing about NSEC5

When I finally grasp NSEC5

backup slides

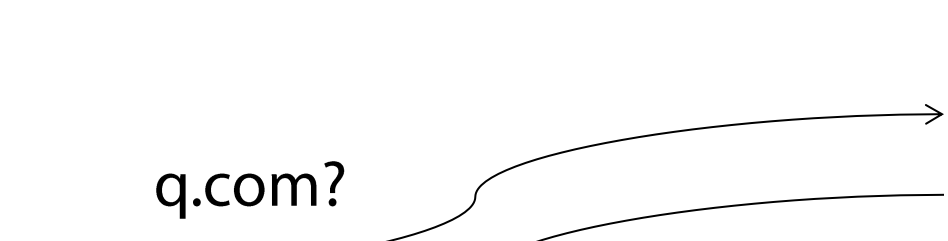
offline zone signing with NSEC3 [RFC5155]

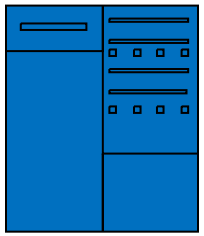


answering queries with NSEC3

Public Zone Signing Key (ZSK):

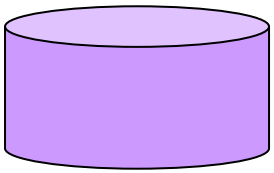
SHA1(q.com**)** = c987b





a.com
c.com
z.com

a1bb5.com
dde45.com



Step 1: Collect

a1bb5.com

dde45.com

23ced.com
a1bb5.com

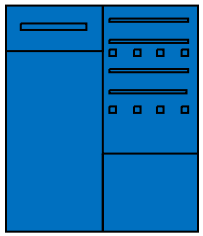
a1bb5.com
dde45.com

dde45.com
23ced.com

offline zone enumeration with NSEC3

Public Zone Signing Key (ZSK):

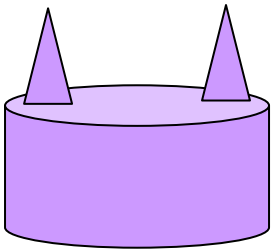
SHA1(r.com**)** = 33c46



a.com
c.com
z.com

r.com?

23ced.com
a1bb5.com



Step 1: Collect

a1bb5.com
dde45.com

Offline dictionary attack

Step 2: Crack

a.com
z.com
c.com

23ced.com
a1bb5.com

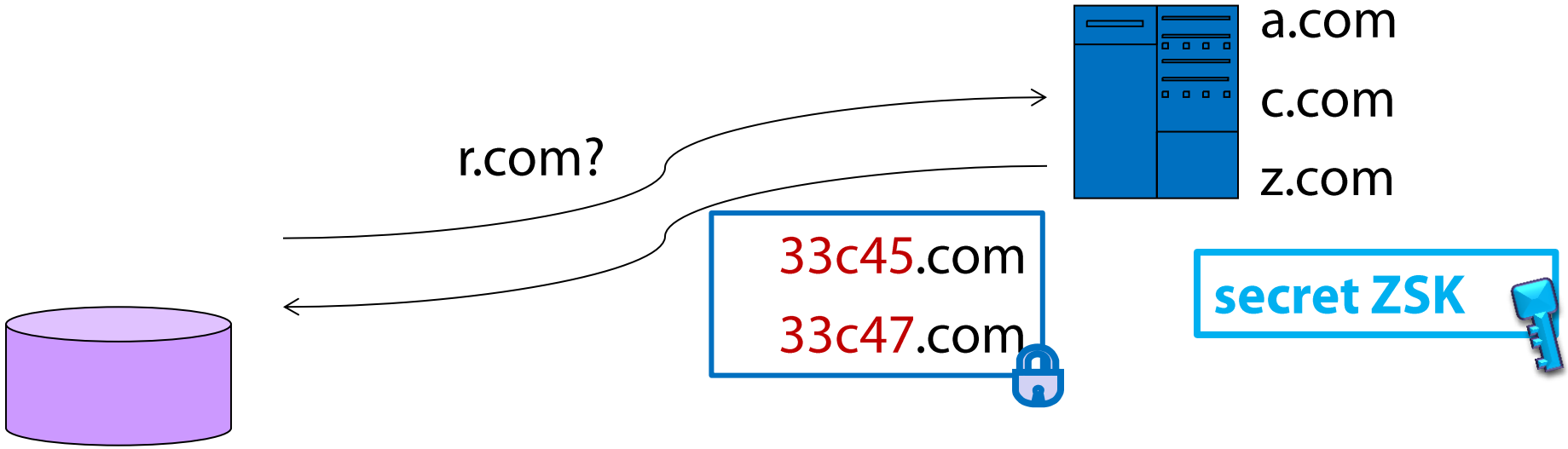
a1bb5.com
dde45.com

dde45.com
23ced.com

online signing stops zone enumeration!

Public Zone Signing Key (ZSK):

SHA1(r.com**)** = 33c46



"NSEC3 White Lies" [RFC7128]