NSEC5: Provably Preventing DNSSEC Zone Enumeration

NDSS Symposium 2015, San Diego, CA. February 10, 2015

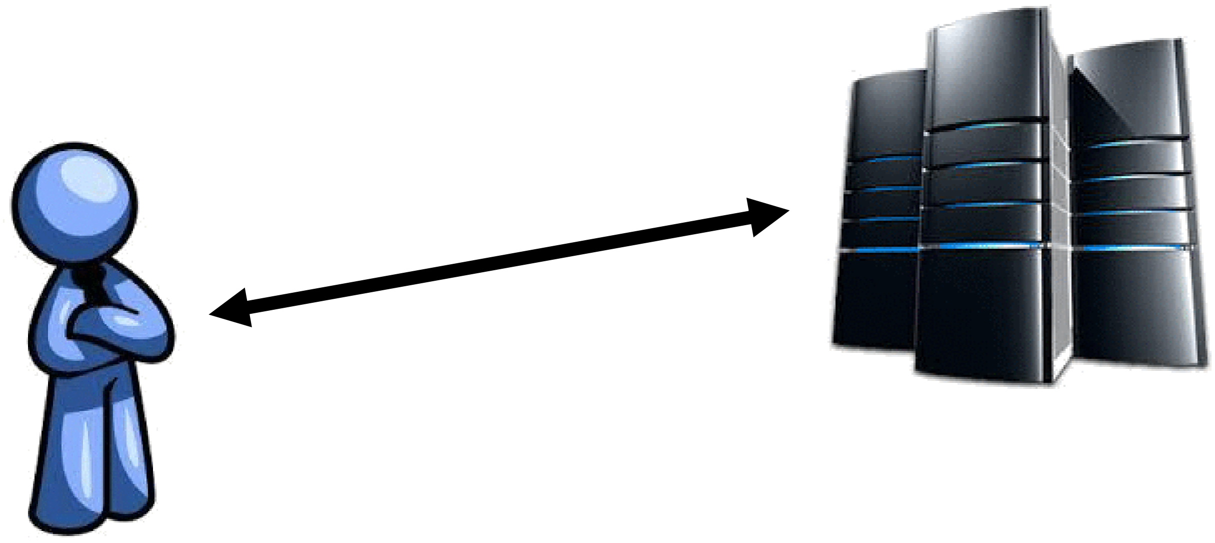
Sharon Goldberg
Dimitrios Papadopoulos
Leonid Reyzin
Sachin Vasant

BOSTON UNIVERSITY

Moni Naor
Asaf Ziv

מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE

DNSSEC model and denial-of-existence

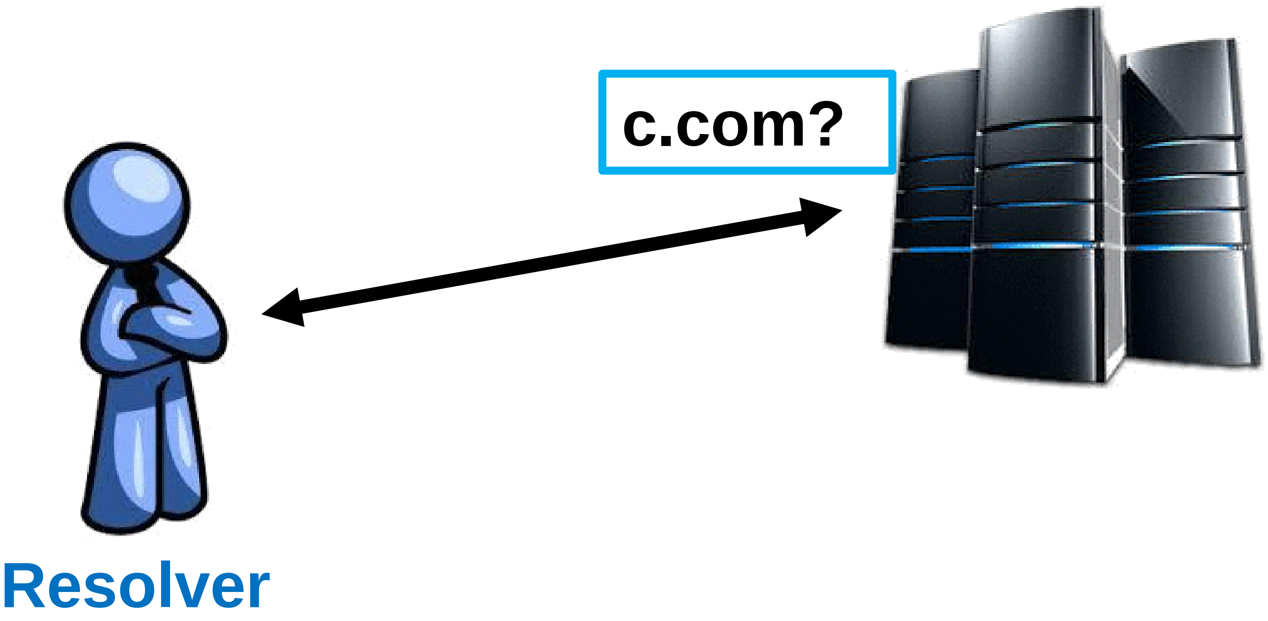


Resolver

Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

DNSSEC model and denial-of-existence



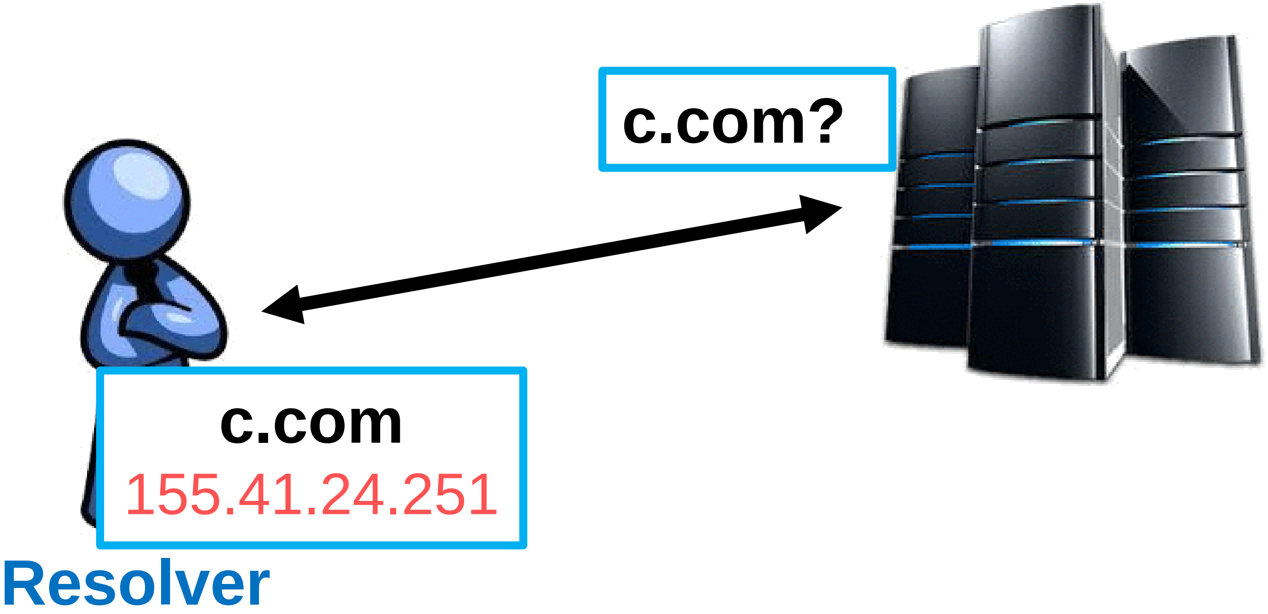
c.com?

Resolver

Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

DNSSEC model and denial-of-existence



c.com?

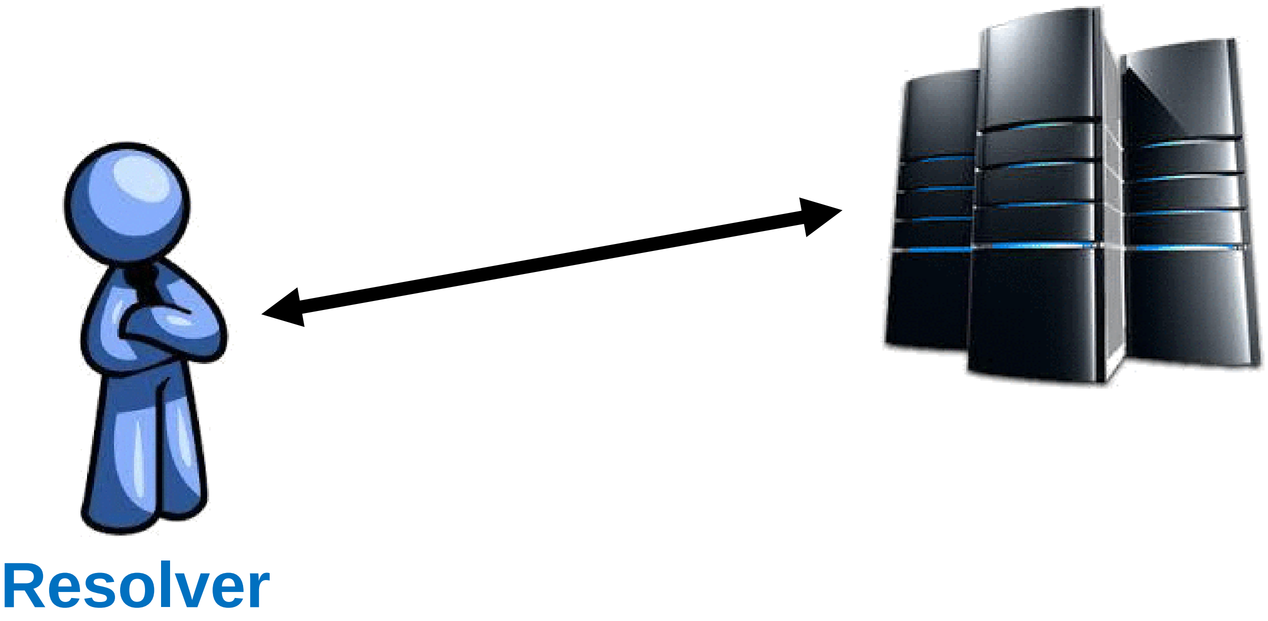
c.com
155.41.24.251

Resolver

Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

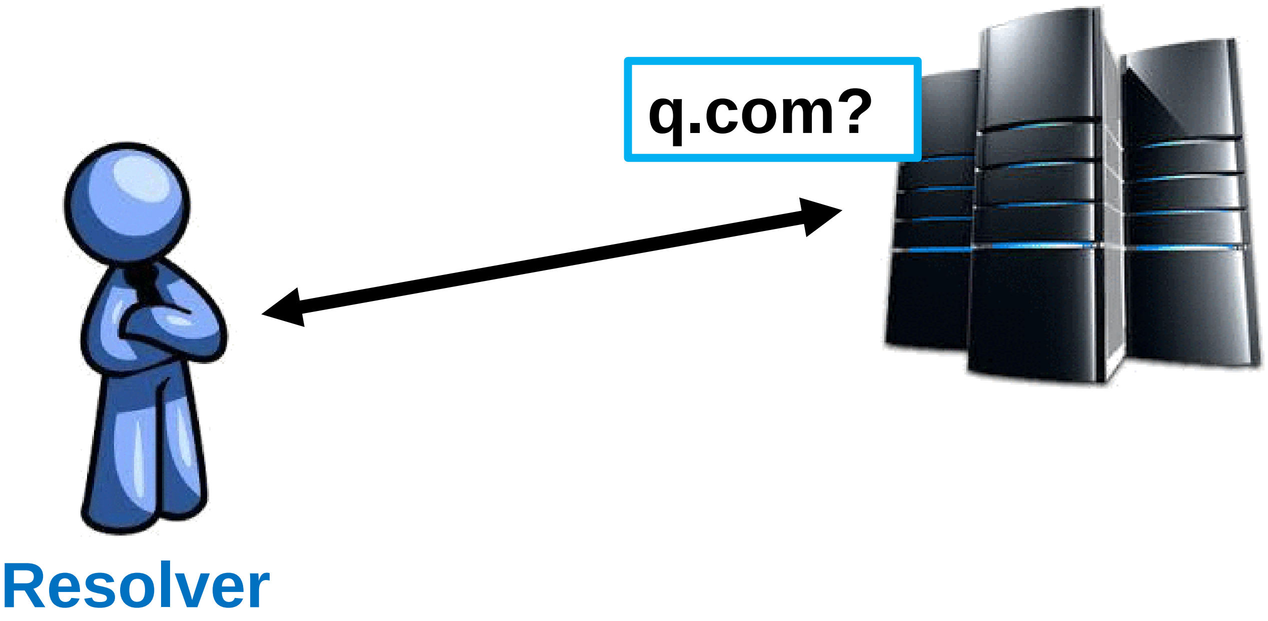
DNSSEC model and denial-of-existence



Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

DNSSEC model and denial-of-existence



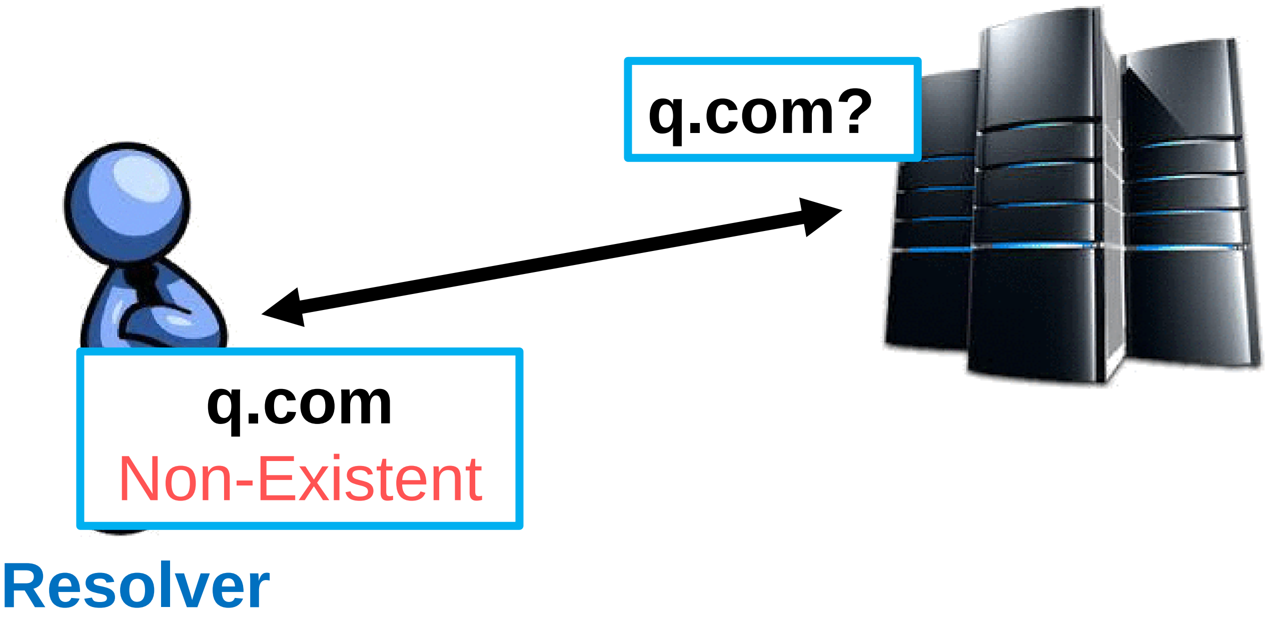
q.com?

Resolver

Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

DNSSEC model and denial-of-existence



q.com?

q.com

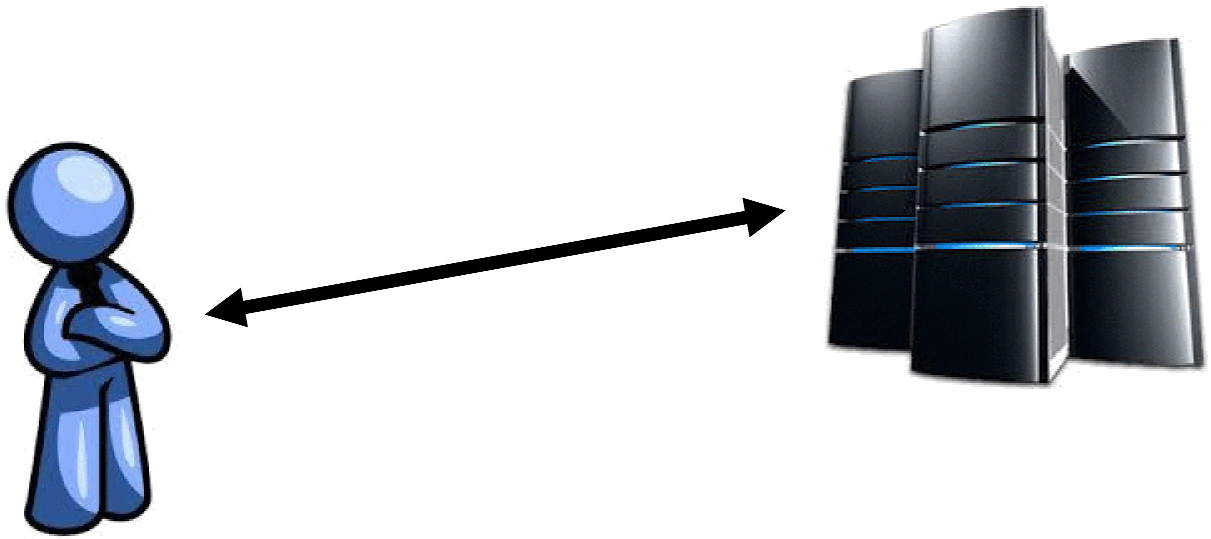
Non-Existent

Resolver

Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

DNSSEC model and denial-of-existence



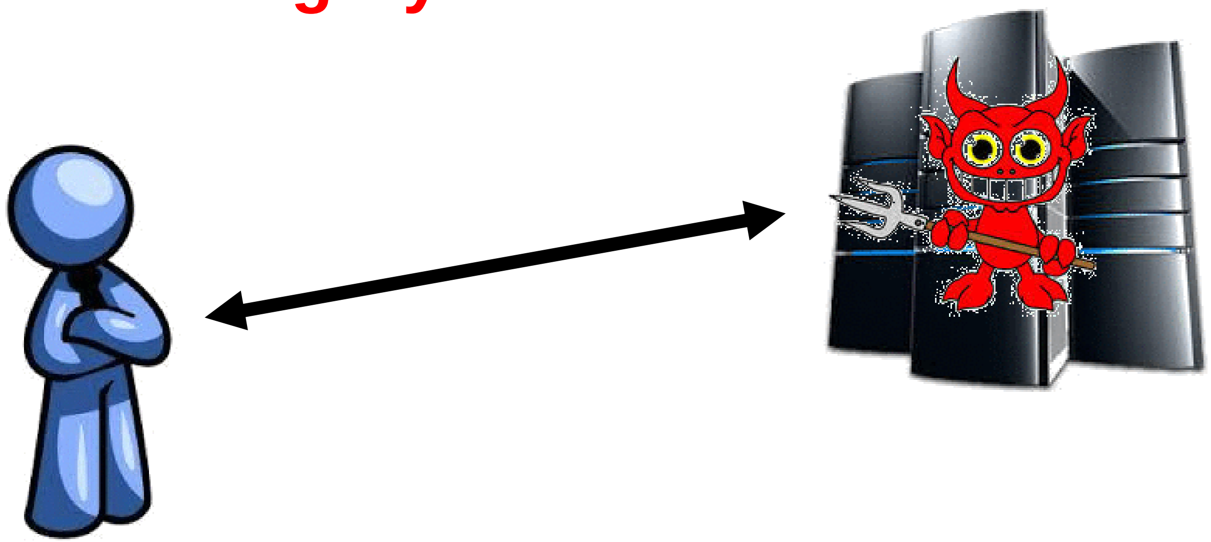
Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

DNSSEC demands Integrity

DNSSEC model and denial-of-existence

Integrity



Zone File

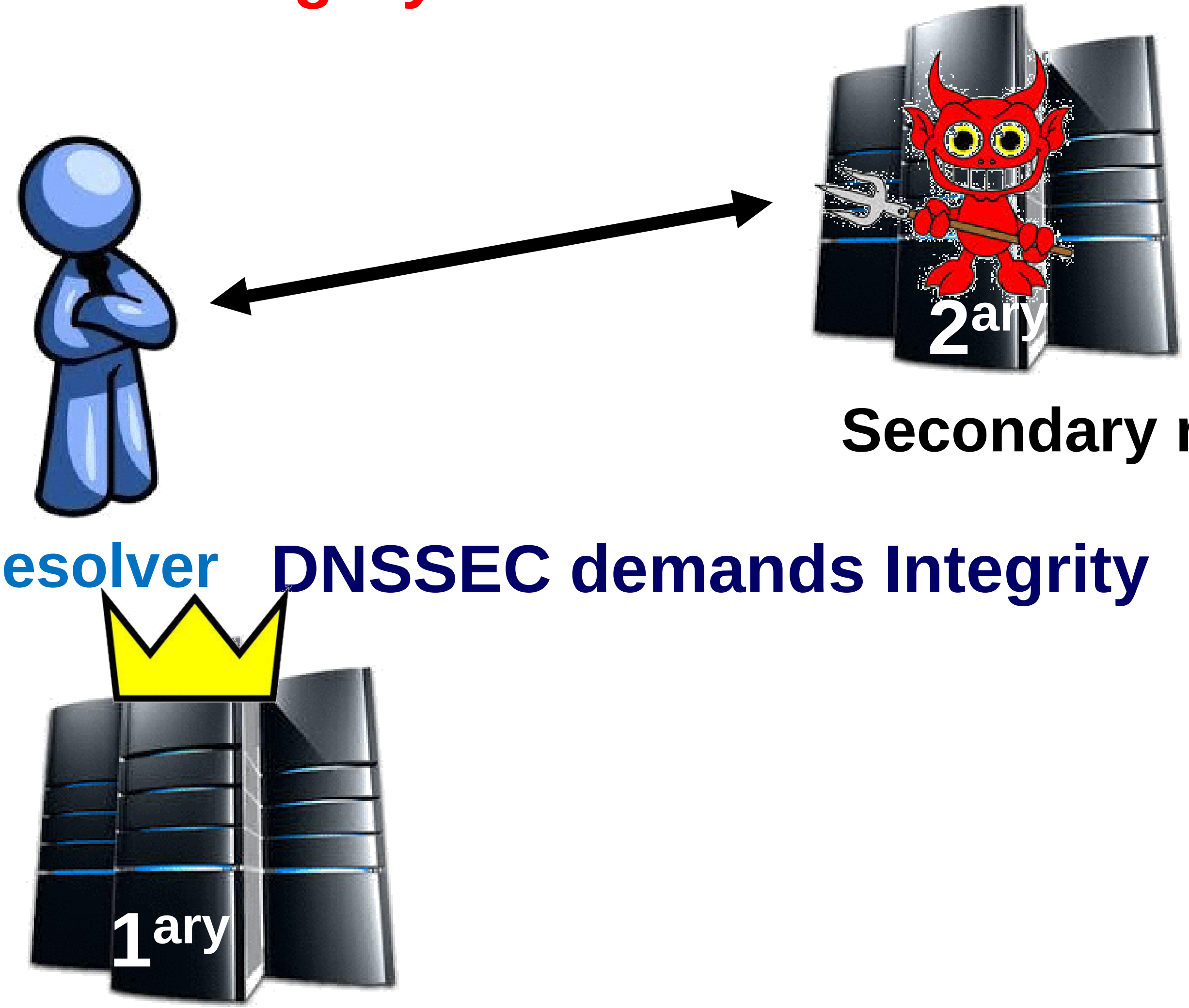
a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

Resolver

DNSSEC demands Integrity

DNSSEC model and denial-of-existence

Integrity



Secondary nameserver

Resolver

Primary nameserver

Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

DNSSEC demands Integrity

DNSSEC model and denial-of-existence

Integrity

Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

Secondary nameserver

Resolver

DNSSEC demands Integrity

🔒 a.com 155.41.24.250

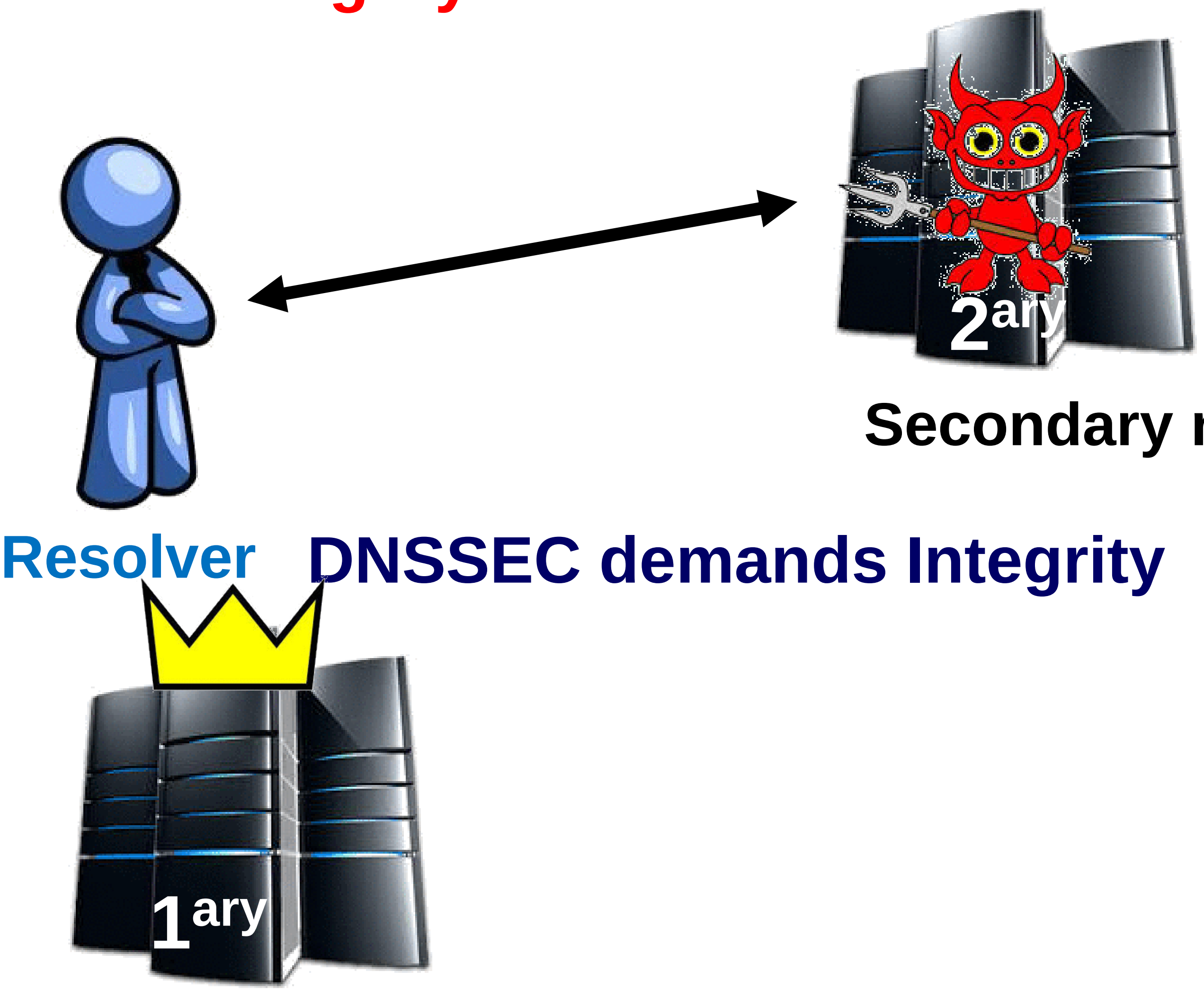
🔒 c.com 155.41.24.251

🔒 z.com 155.41.24.252

Primary nameserver

DNSSEC model and denial-of-existence

Integrity



Secondary nameserver

Resolver

DNSSEC demands Integrity

Primary nameserver

Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

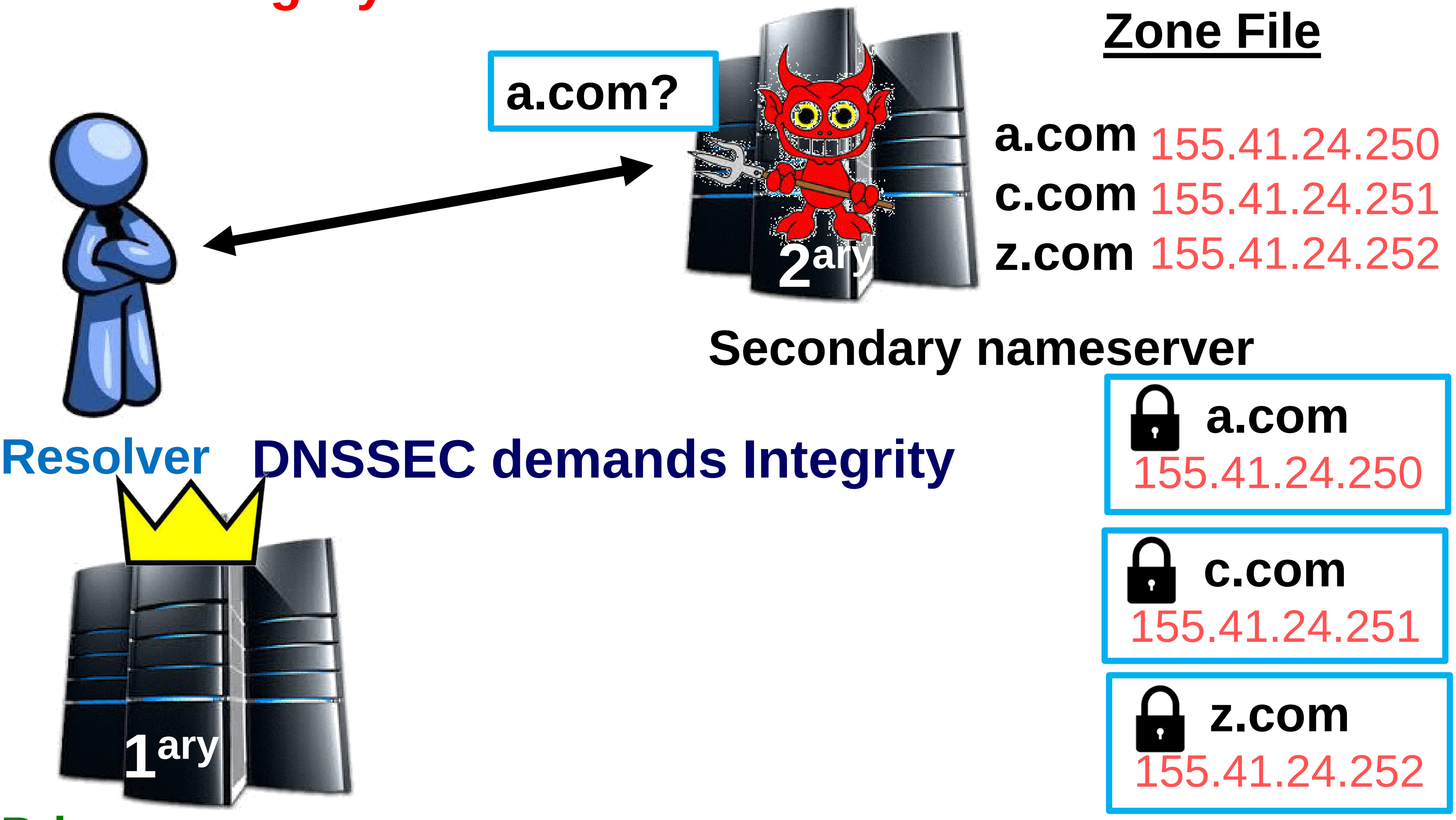
🔒 a.com
155.41.24.250

🔒 c.com
155.41.24.251

🔒 z.com
155.41.24.252

DNSSEC model and denial-of-existence

Integrity



a.com?

Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

Secondary nameserver

Resolver

DNSSEC demands Integrity

a.com 155.41.24.250

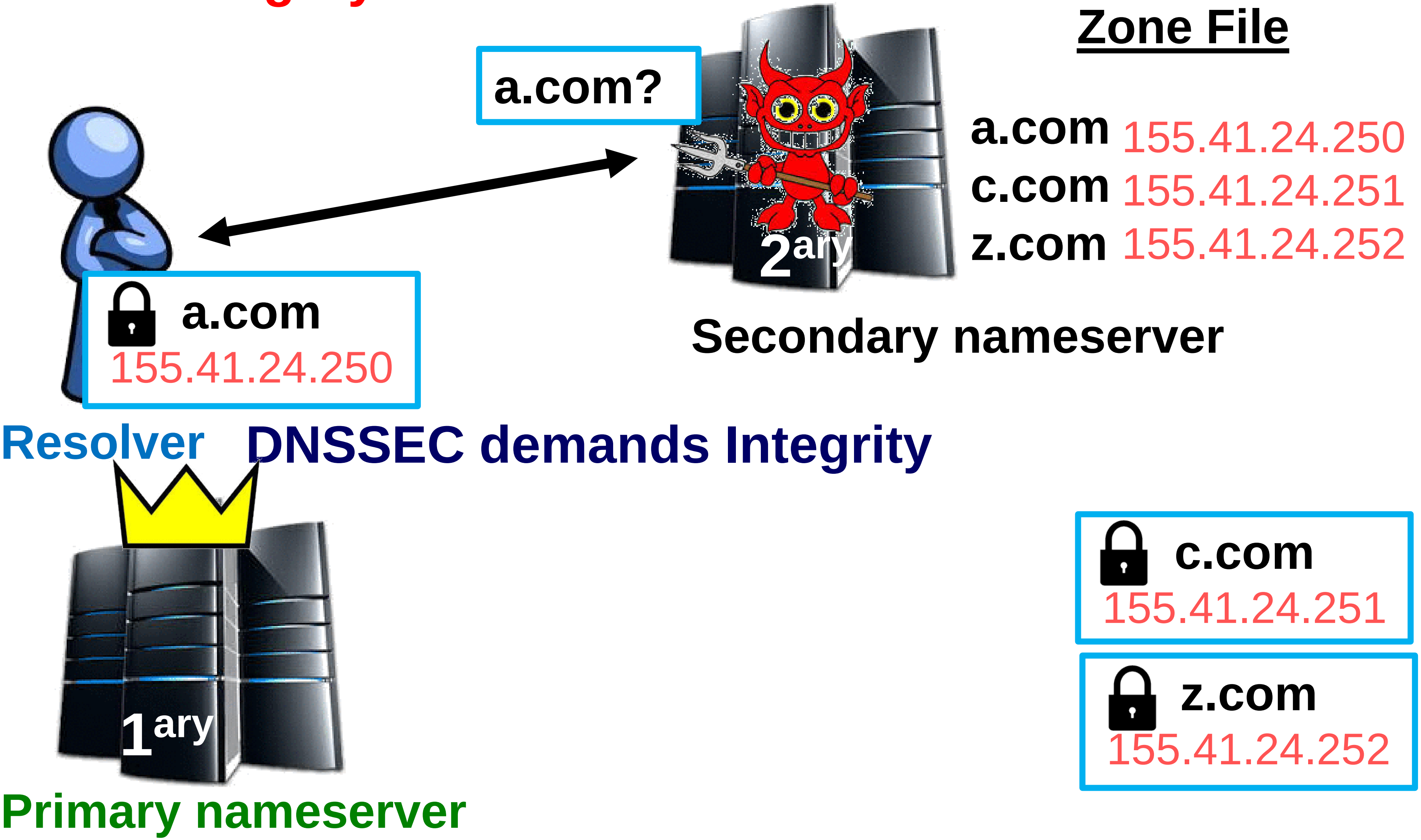
c.com 155.41.24.251

z.com 155.41.24.252

Primary nameserver

DNSSEC model and denial-of-existence

Integrity



a.com?

Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

2ary

Secondary nameserver

a.com
155.41.24.250

Resolver

DNSSEC demands Integrity

1ary

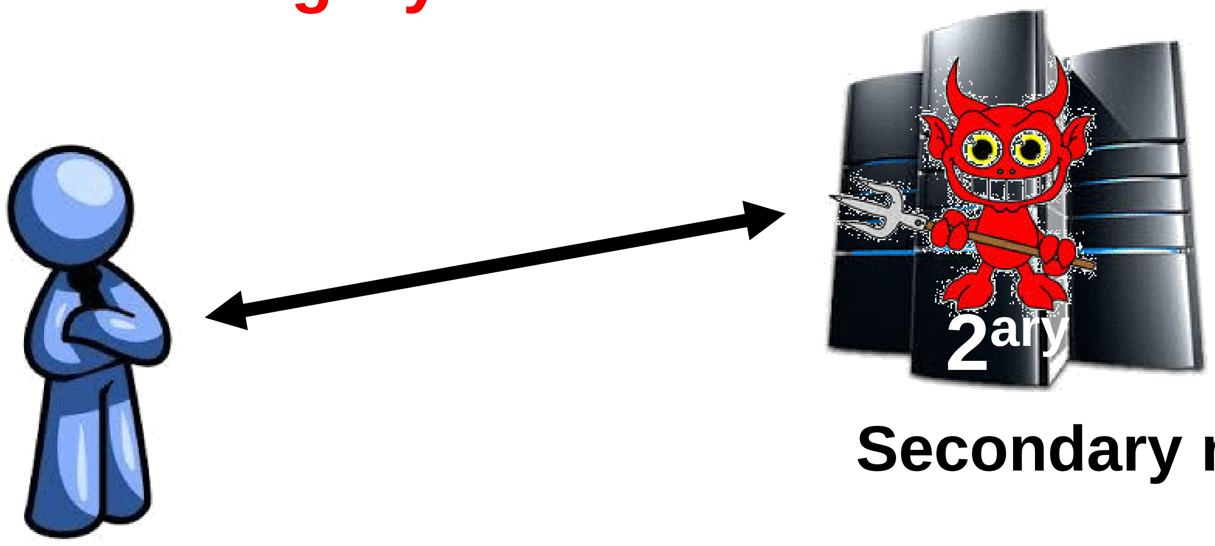
Primary nameserver

c.com
155.41.24.251

z.com
155.41.24.252

DNSSEC model and denial-of-existence

Integrity



Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

Secondary nameserver

Resolver

DNSSEC demands Integrity

?

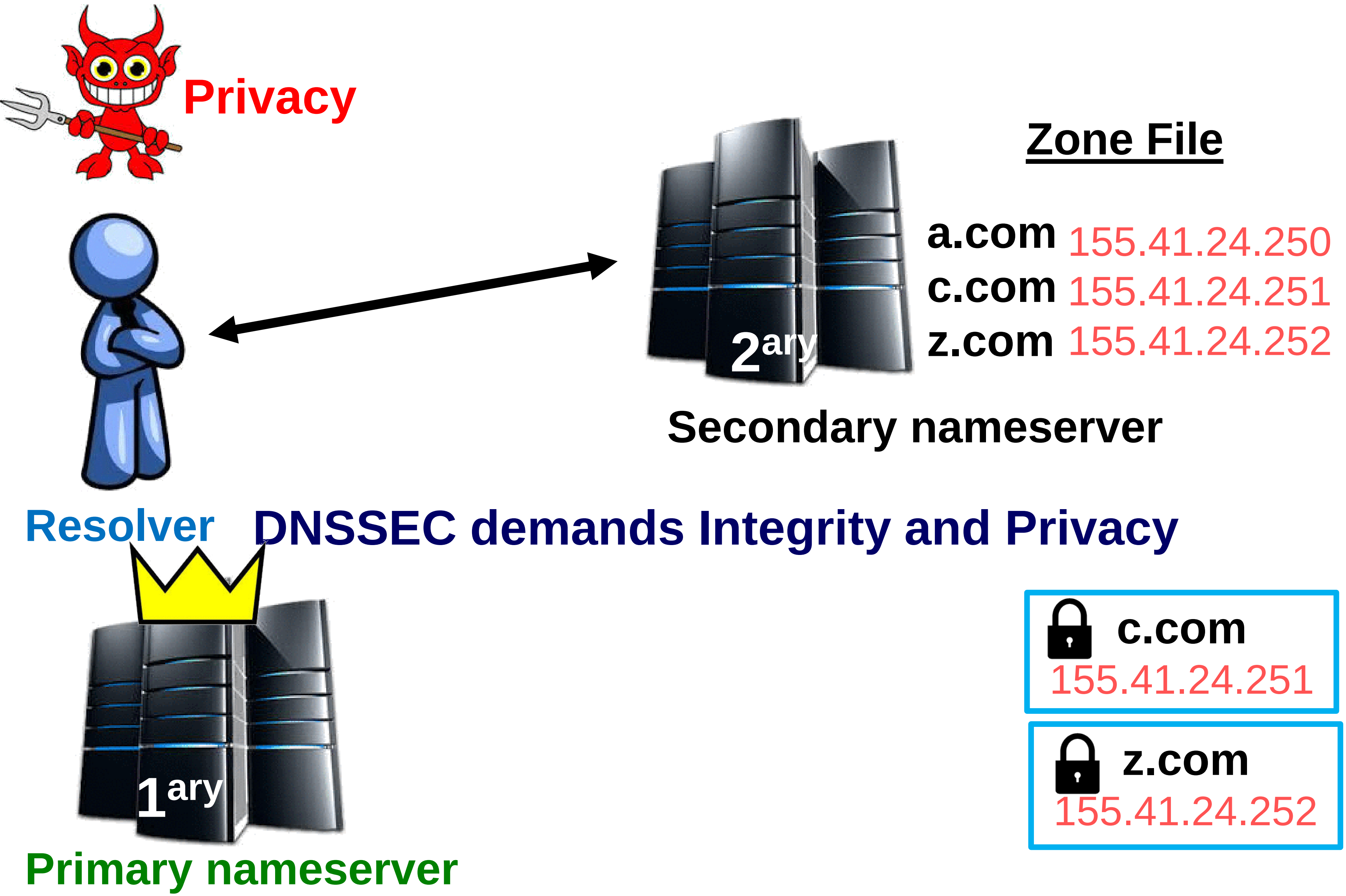
q.com
Non-Existent

c.com
155.41.24.251

z.com
155.41.24.252

Primary nameserver

DNSSEC model and denial-of-existence



Privacy

Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

Secondary nameserver

Resolver

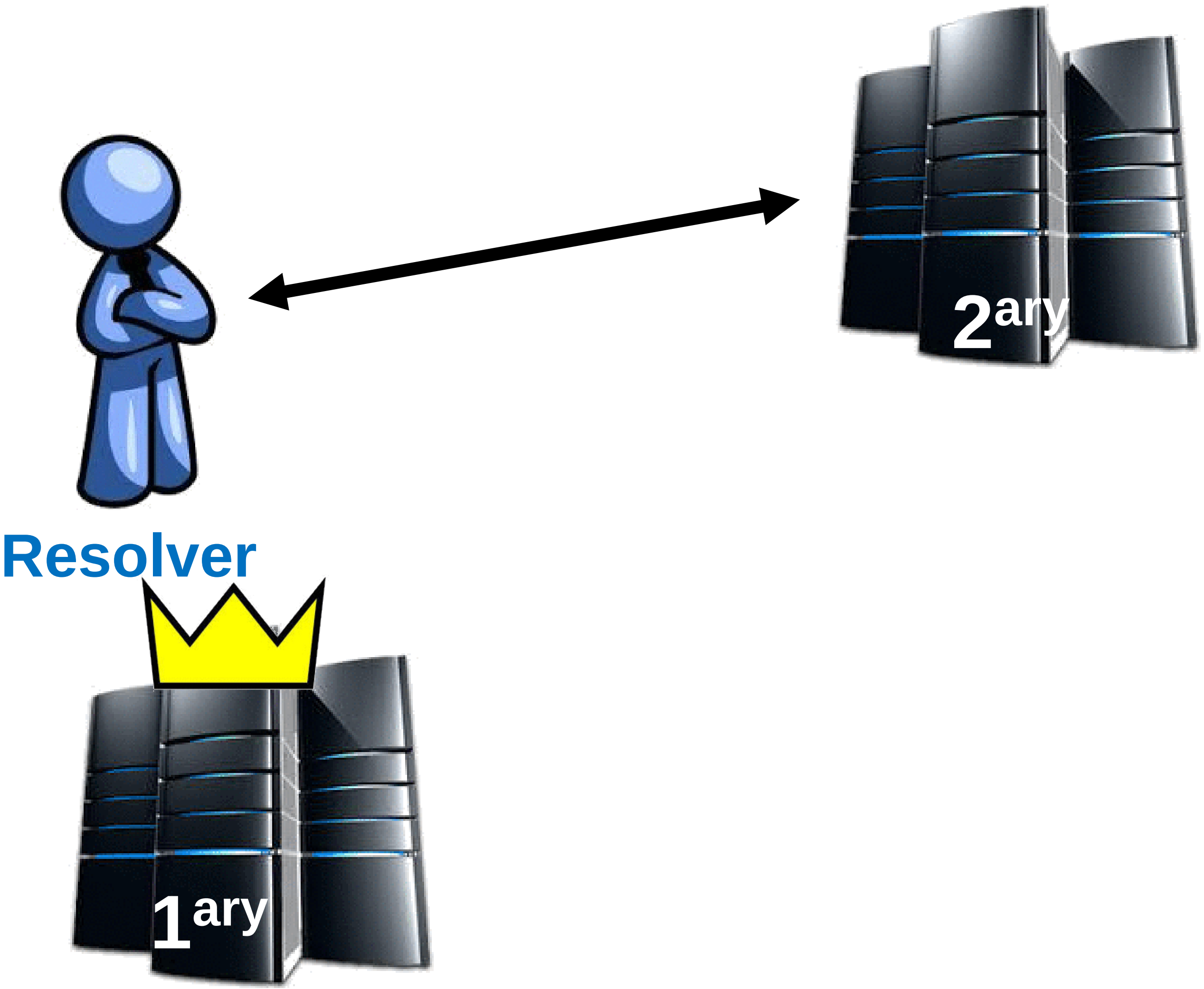
DNSSEC demands Integrity and Privacy

c.com
155.41.24.251

z.com
155.41.24.252

Primary nameserver

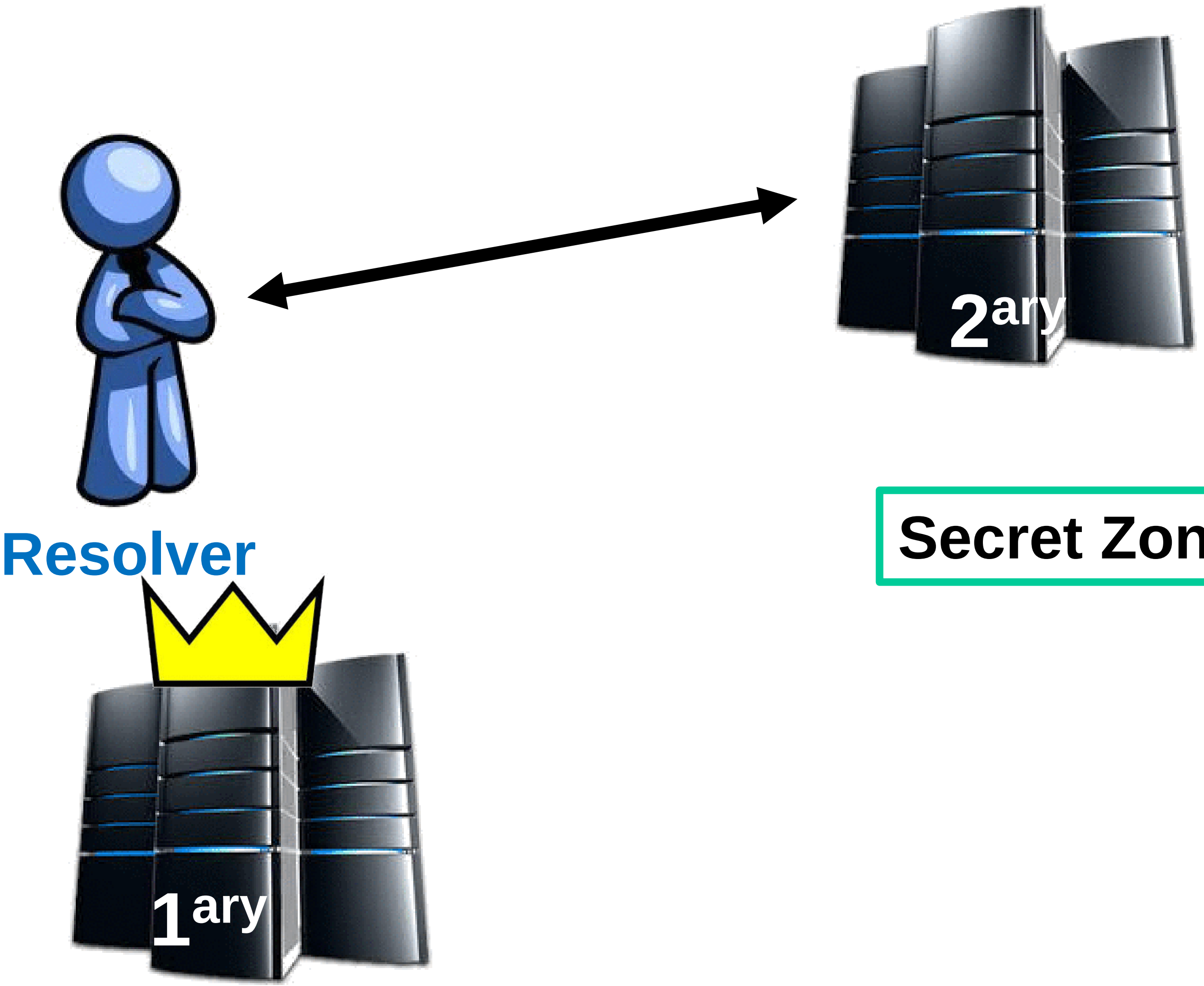
RFC 4470 – Online signing



Zone Names

a.com
c.com
z.com

RFC 4470 – Online signing

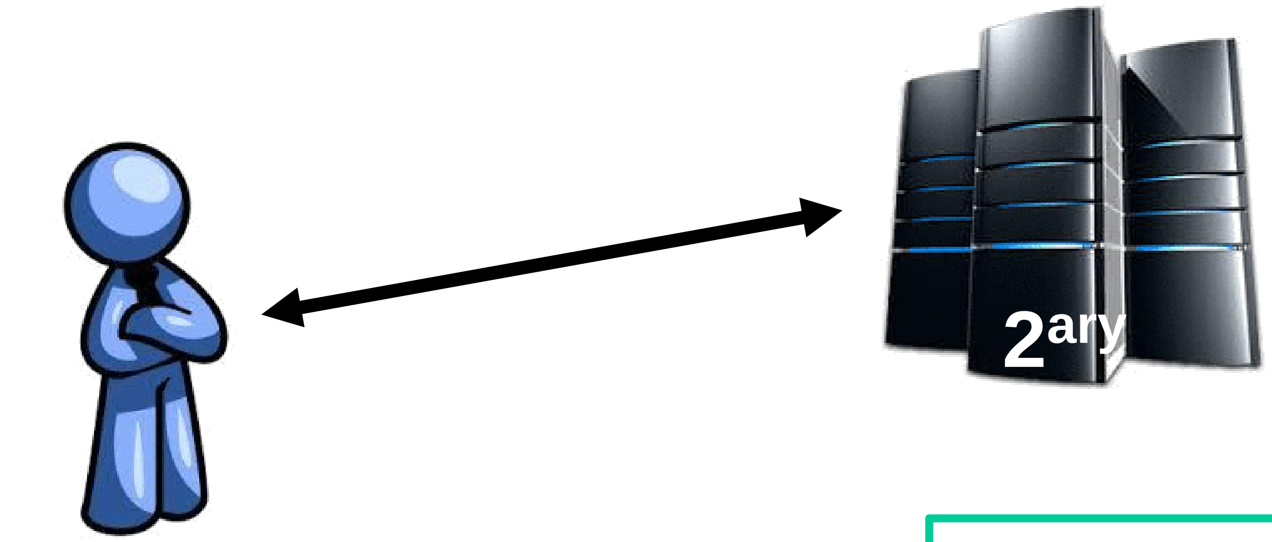


Zone Names

a.com
c.com
z.com

Secret Zone Signing Key

RFC 4470 – Online signing



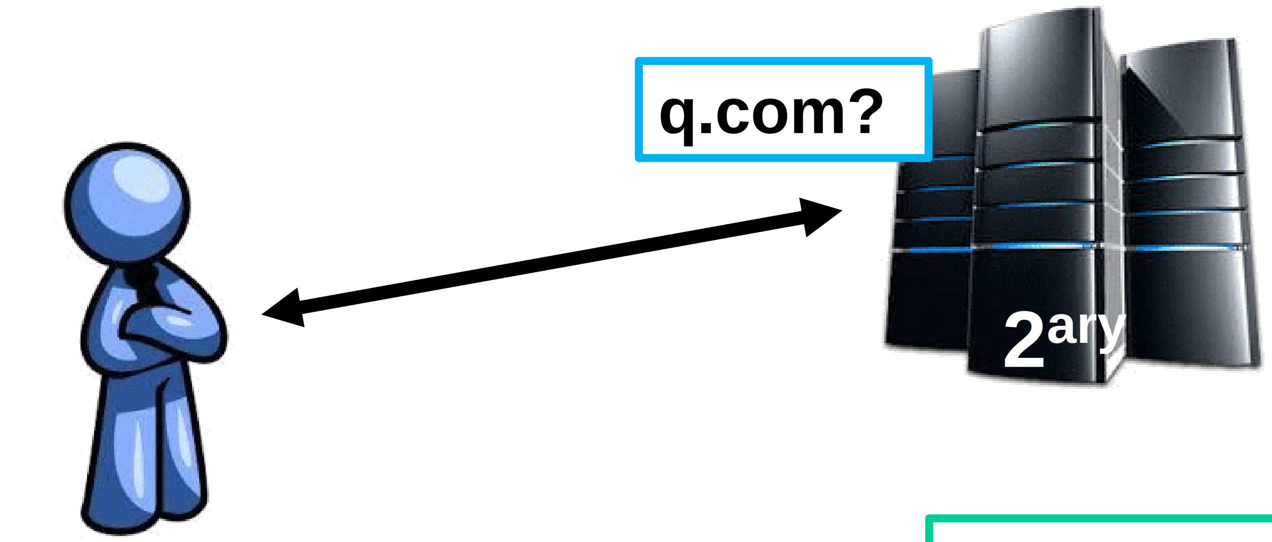
Resolver

Zone Names

a.com
c.com
z.com

Secret Zone Signing Key

RFC 4470 – Online signing



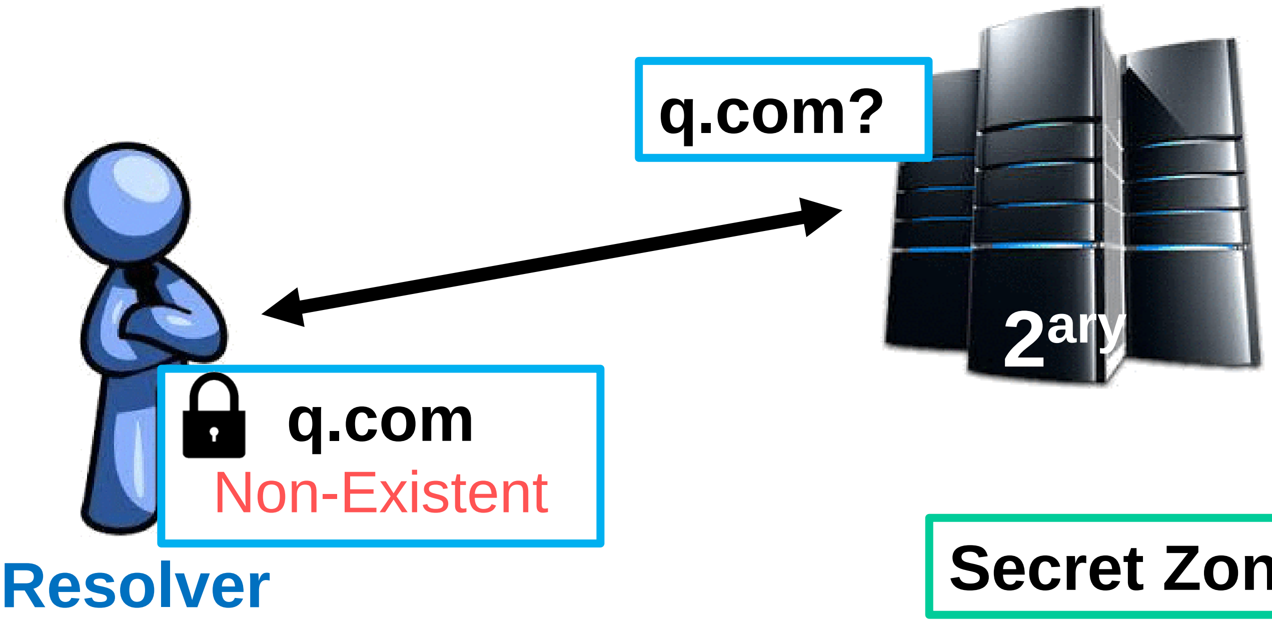
Resolver

Zone Names

a.com
c.com
z.com

Secret Zone Signing Key

RFC 4470 – Online signing



q.com?

q.com
Non-Existent

2^{ary}

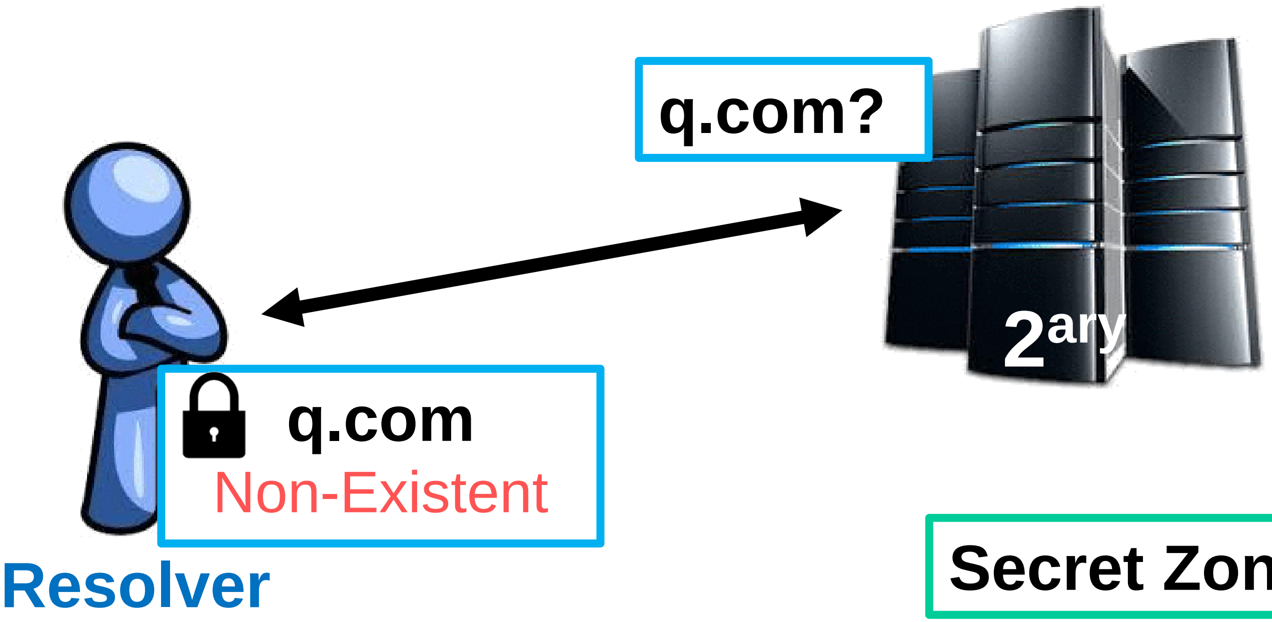
Resolver

Zone Names

a.com
c.com
z.com

Secret Zone Signing Key

RFC 4470 – Online signing



q.com?

🔒 q.com

Non-Existent

Resolver

2^{ary}

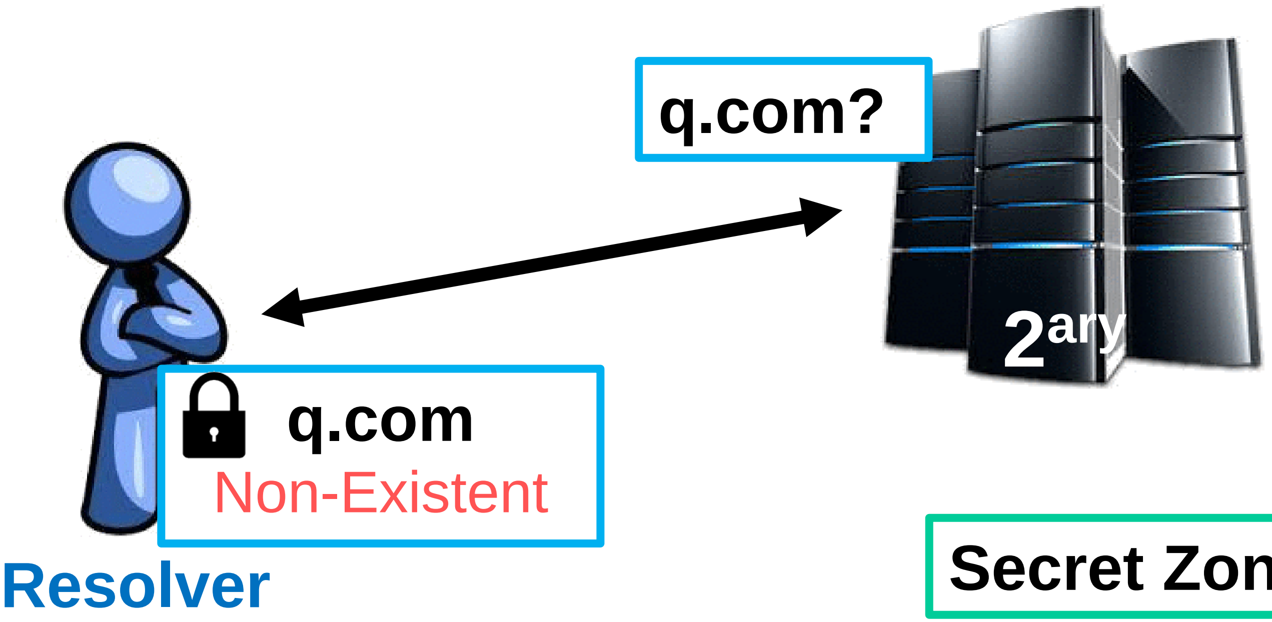
Zone Names

a.com
c.com
z.com

Secret Zone Signing Key

Integrity?

RFC 4470 – Online signing



q.com?

q.com

Non-Existent

2^{ary}

Resolver

Zone Names

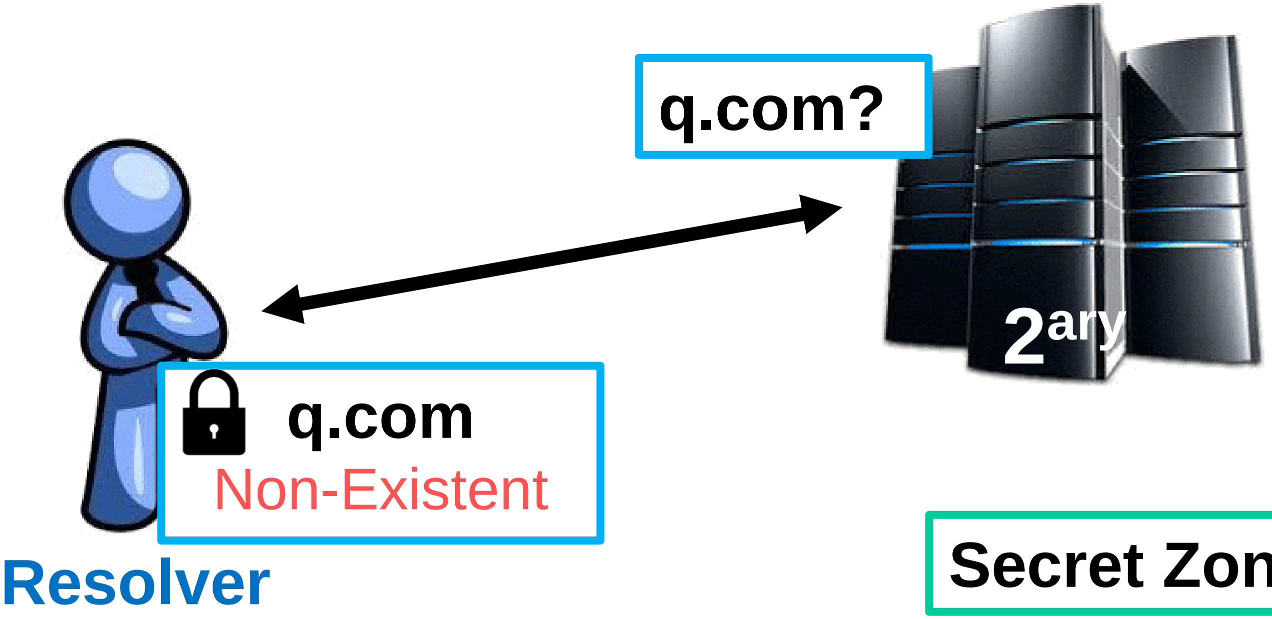
a.com
c.com
z.com

Secret Zone Signing Key

Integrity?

Privacy?

RFC 4470 – Online signing



q.com?

🔒 q.com
Non-Existent

Resolver

2^{ary}

Zone Names

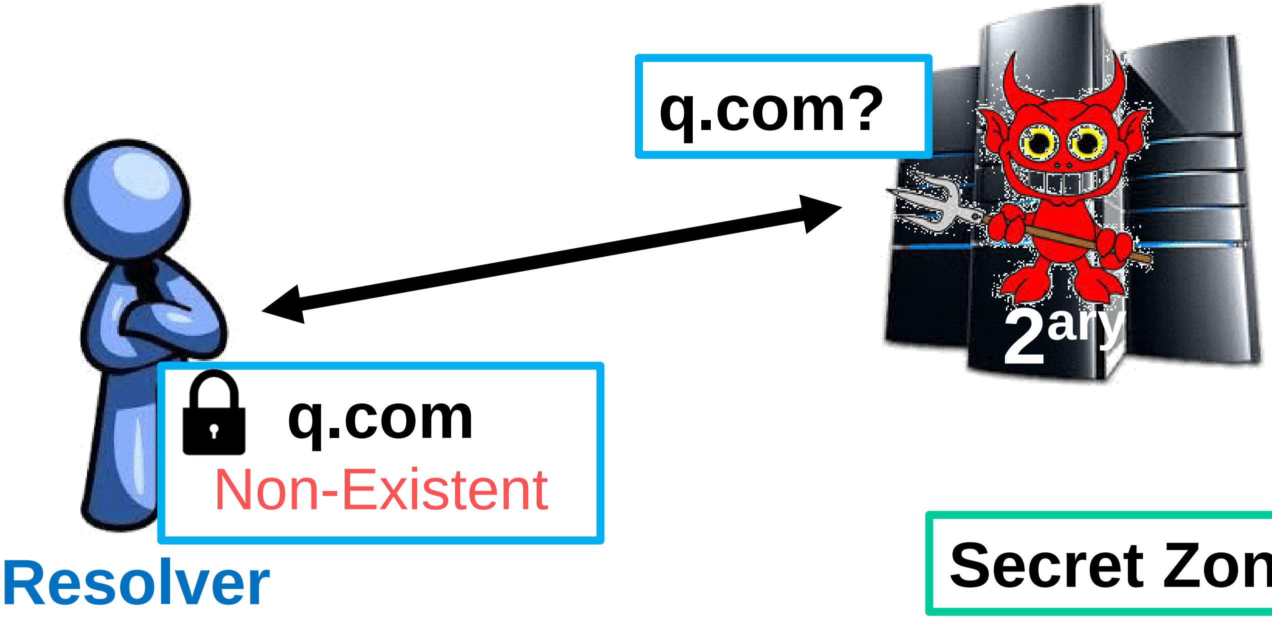
a.com
c.com
z.com

Secret Zone Signing Key

Integrity?

Privacy? **Yes!**

RFC 4470 – Online signing



q.com?

q.com

Non-Existent

Resolver

Zone Names

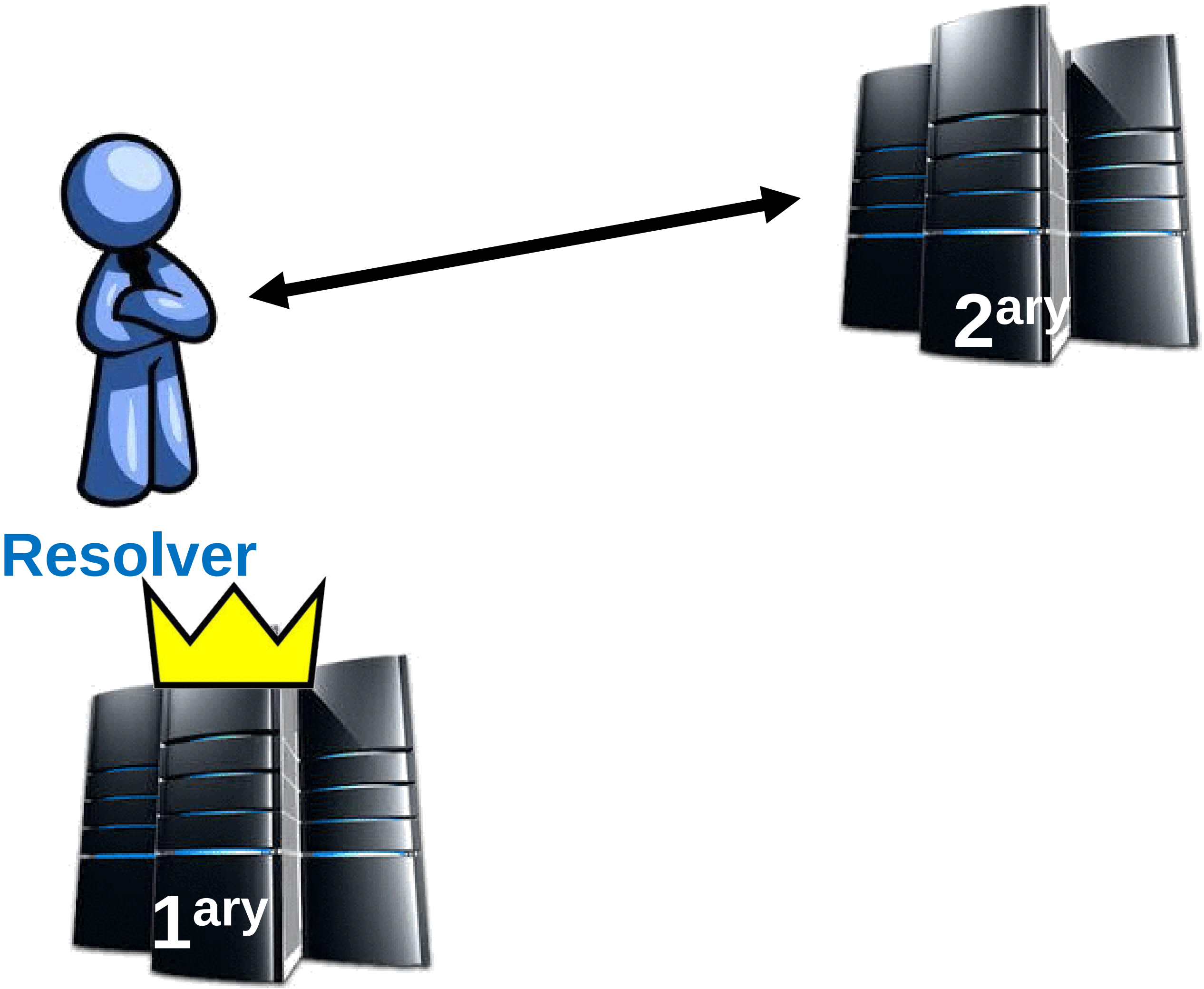
a.com
c.com
z.com

Secret Zone Signing Key

Integrity? Only if we trust Secondary nameserver!

Privacy? Yes!

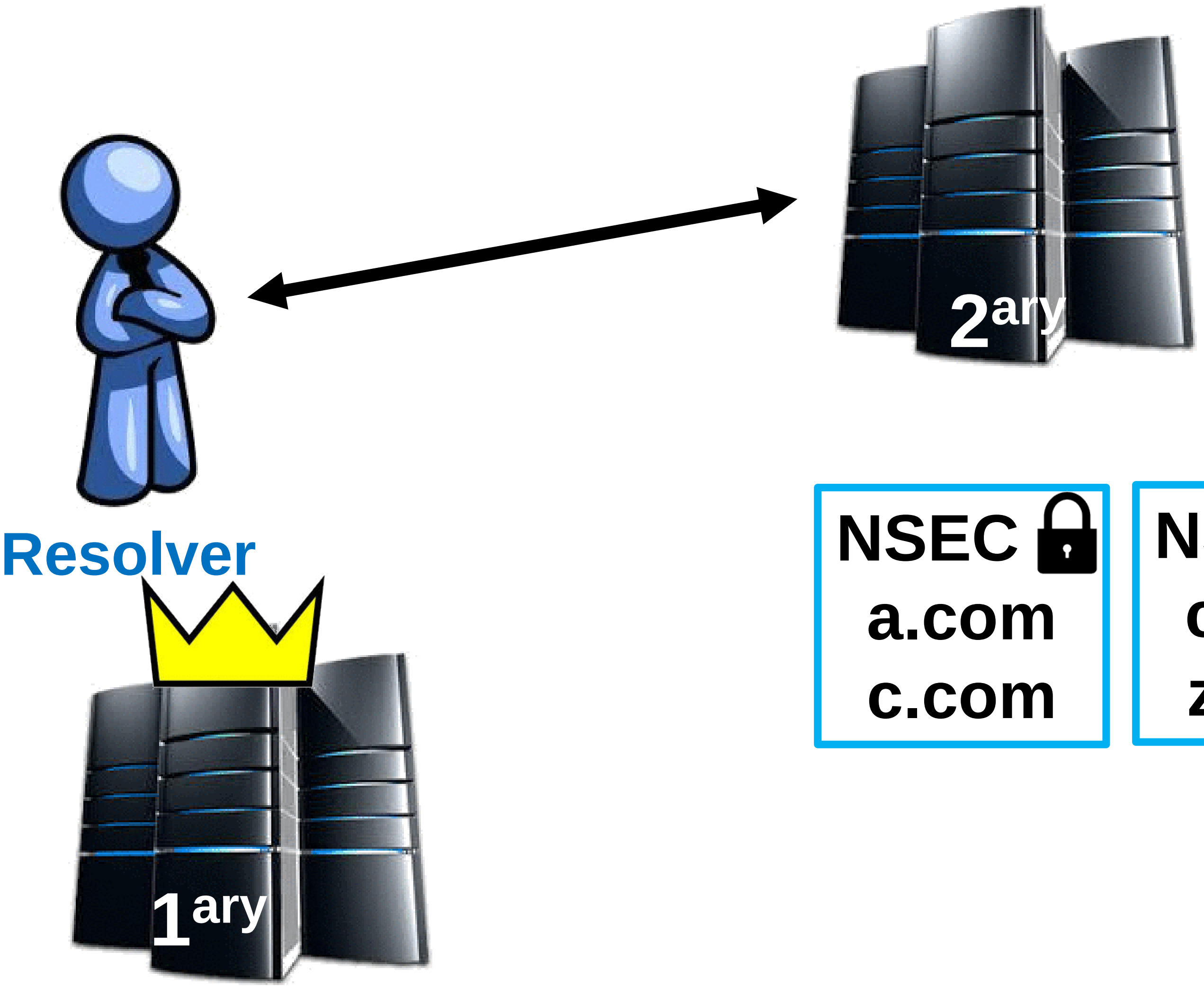
RFC 4034 – NSEC



Zone Names

a.com
c.com
z.com

RFC 4034 – NSEC



Zone Names

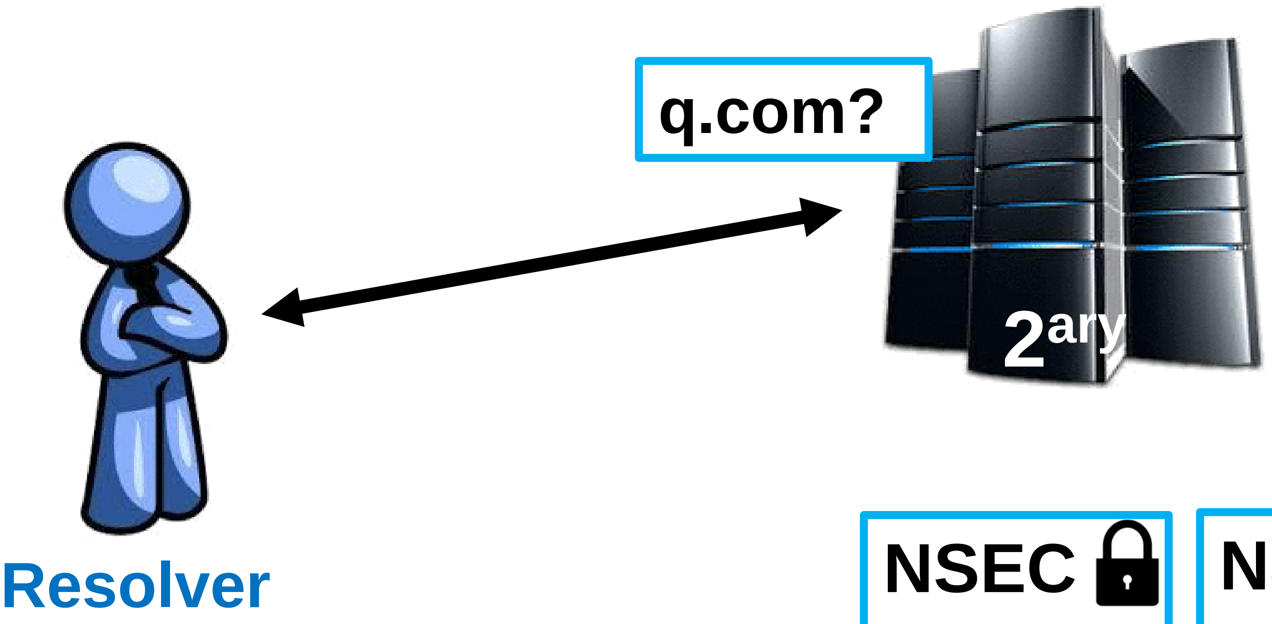
a.com
c.com
z.com

NSEC 🔒
a.com
c.com

NSEC 🔒
c.com
z.com

NSEC 🔒
z.com
a.com

RFC 4034 – NSEC

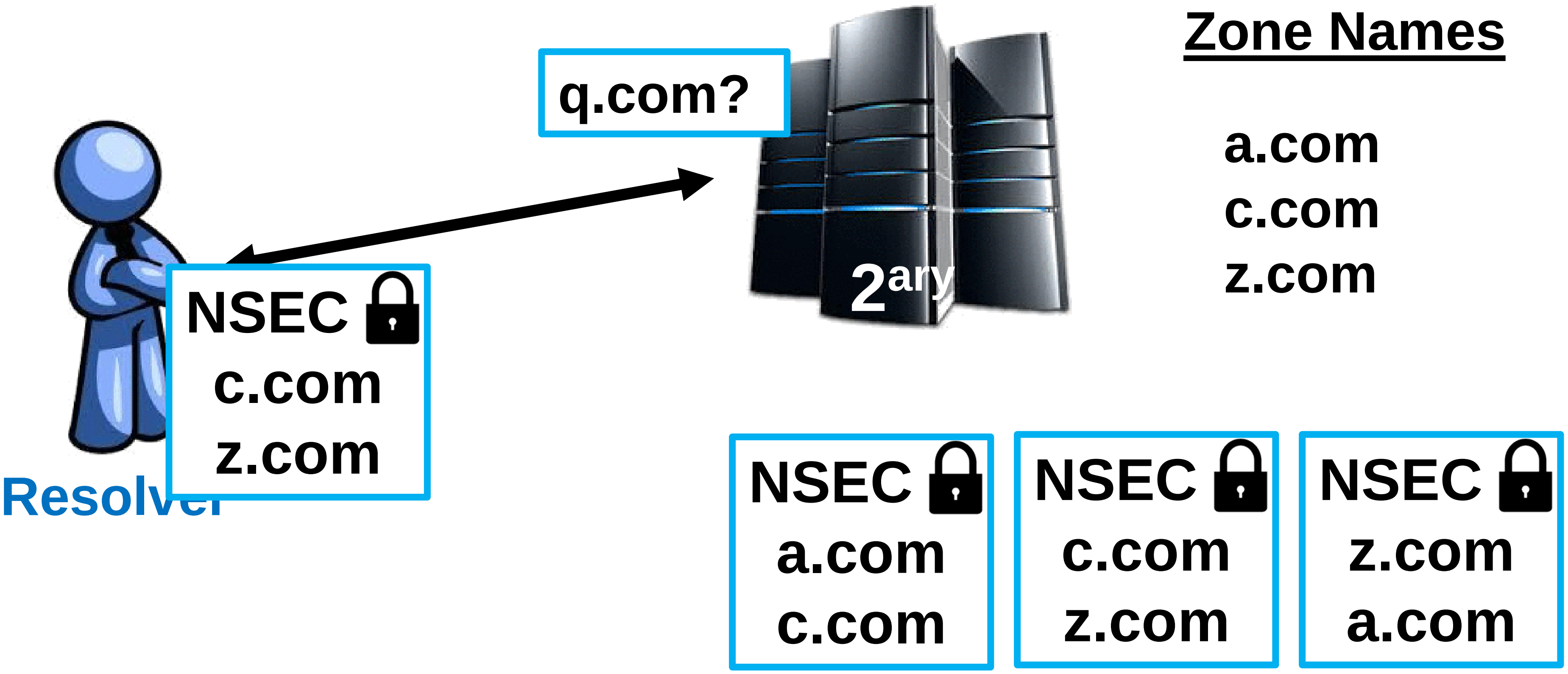


Zone Names

a.com
c.com
z.com

NSEC 🔒 **a.com** **c.com**	**NSEC 🔒** **c.com** **z.com**	**NSEC 🔒** **z.com** **a.com**

RFC 4034 – NSEC



q.com?

NSEC 🔒
c.com
z.com

Resolver

2ary

Zone Names

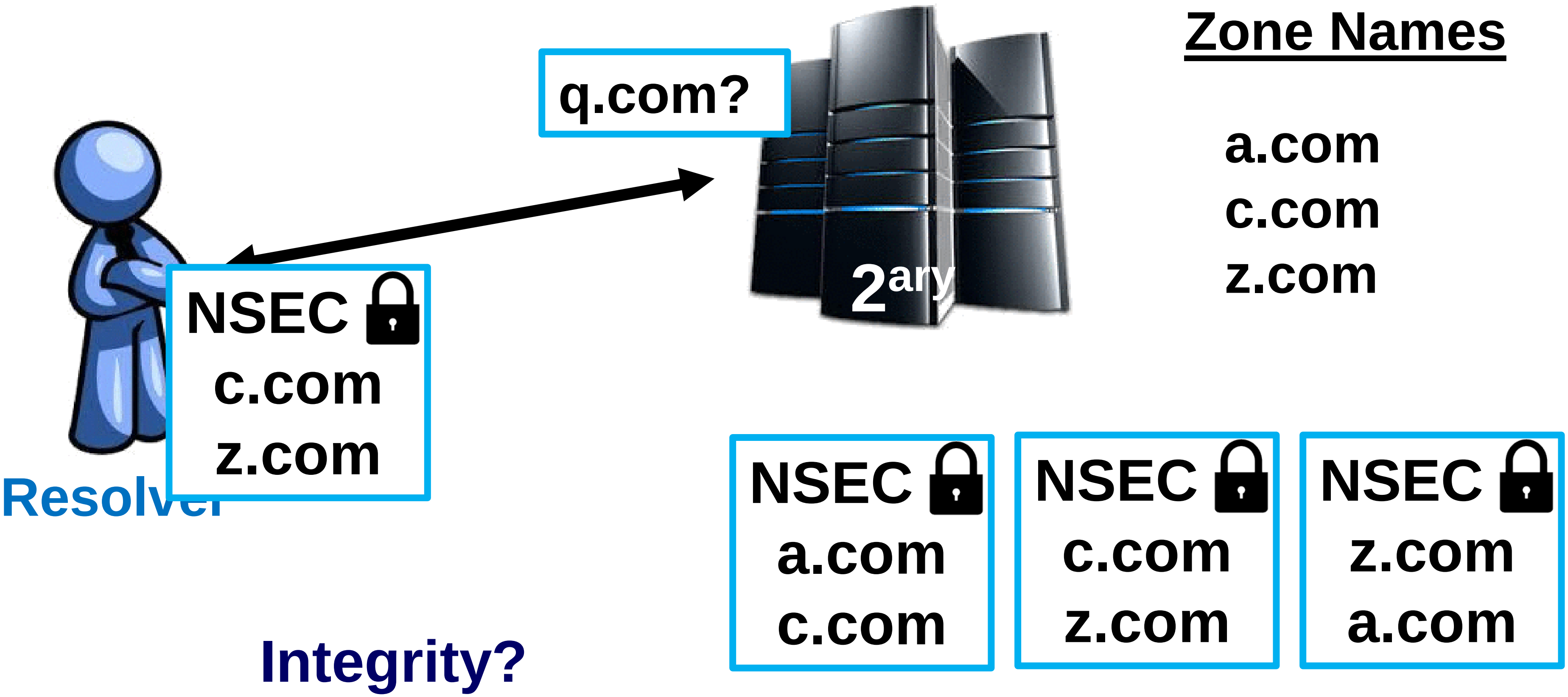
a.com
c.com
z.com

NSEC 🔒
a.com
c.com

NSEC 🔒
c.com
z.com

NSEC 🔒
z.com
a.com

RFC 4034 – NSEC



q.com?

NSEC 🔒
c.com
z.com

Resolver

2^{ary}

Zone Names

a.com
c.com
z.com

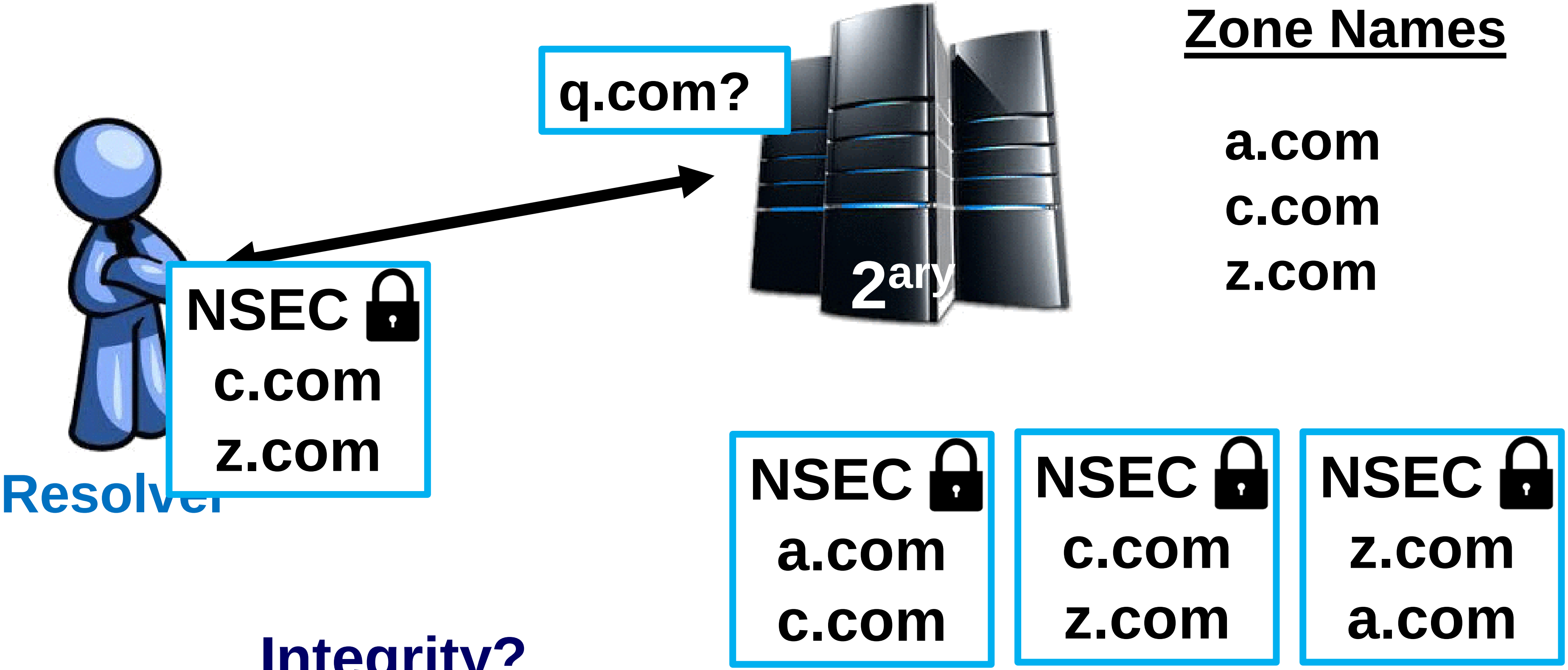
NSEC 🔒
a.com
c.com

NSEC 🔒
c.com
z.com

NSEC 🔒
z.com
a.com

Integrity?

RFC 4034 – NSEC



q.com?

NSEC
c.com
z.com

Resolver

2ary

Zone Names

a.com
c.com
z.com

NSEC
a.com
c.com

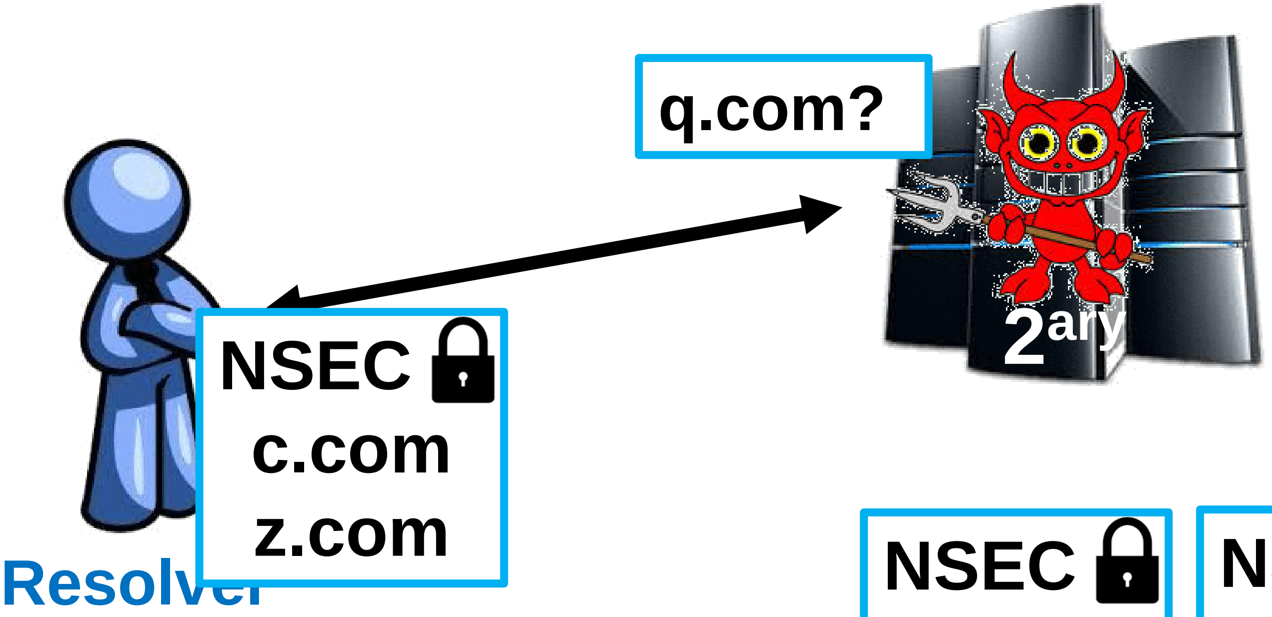
NSEC
c.com
z.com

NSEC
z.com
a.com

Integrity?

Privacy?

RFC 4034 – NSEC



Zone Names

a.com
c.com
z.com

NSEC 🔒
a.com
c.com

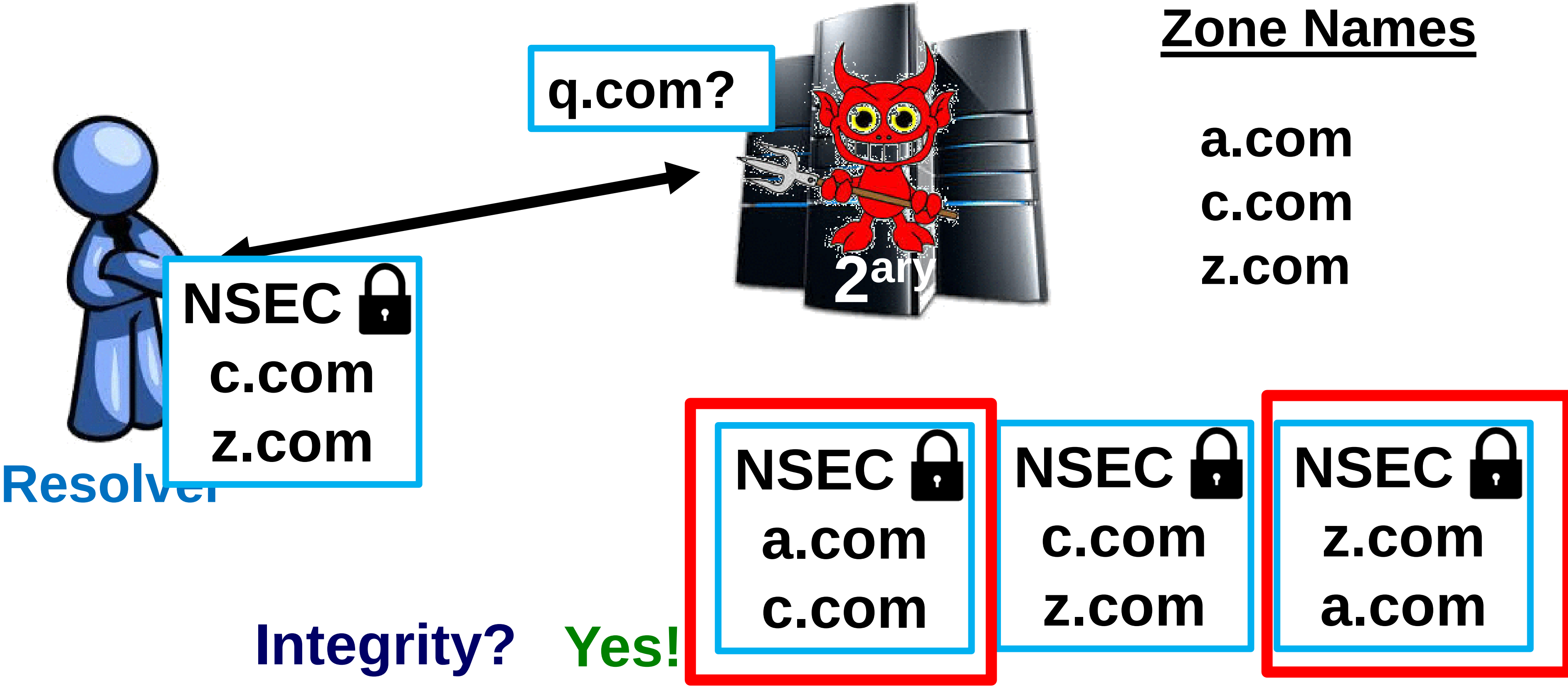
NSEC 🔒
c.com
z.com

NSEC 🔒
z.com
a.com

Integrity? **Yes!**

Privacy?

RFC 4034 – NSEC



q.com?

NSEC
c.com
z.com

Resolver

2ary

Zone Names

a.com
c.com
z.com

NSEC
a.com
c.com

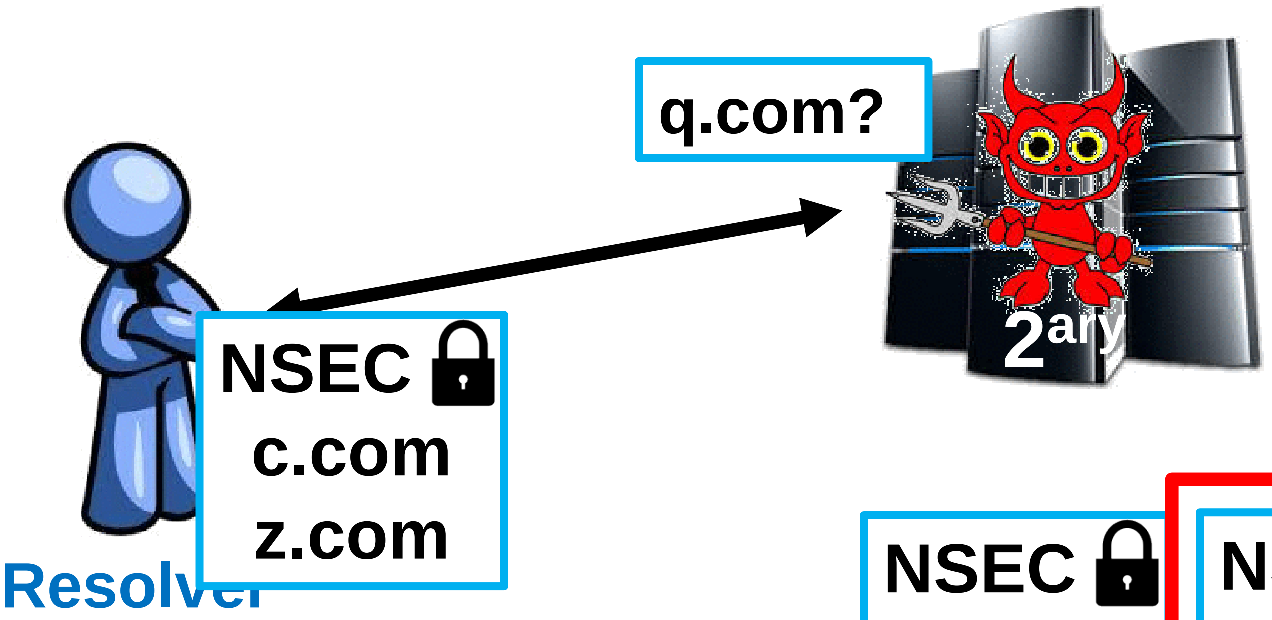
NSEC
c.com
z.com

NSEC
z.com
a.com

Integrity? Yes!

Privacy?

RFC 4034 – NSEC



Zone Names

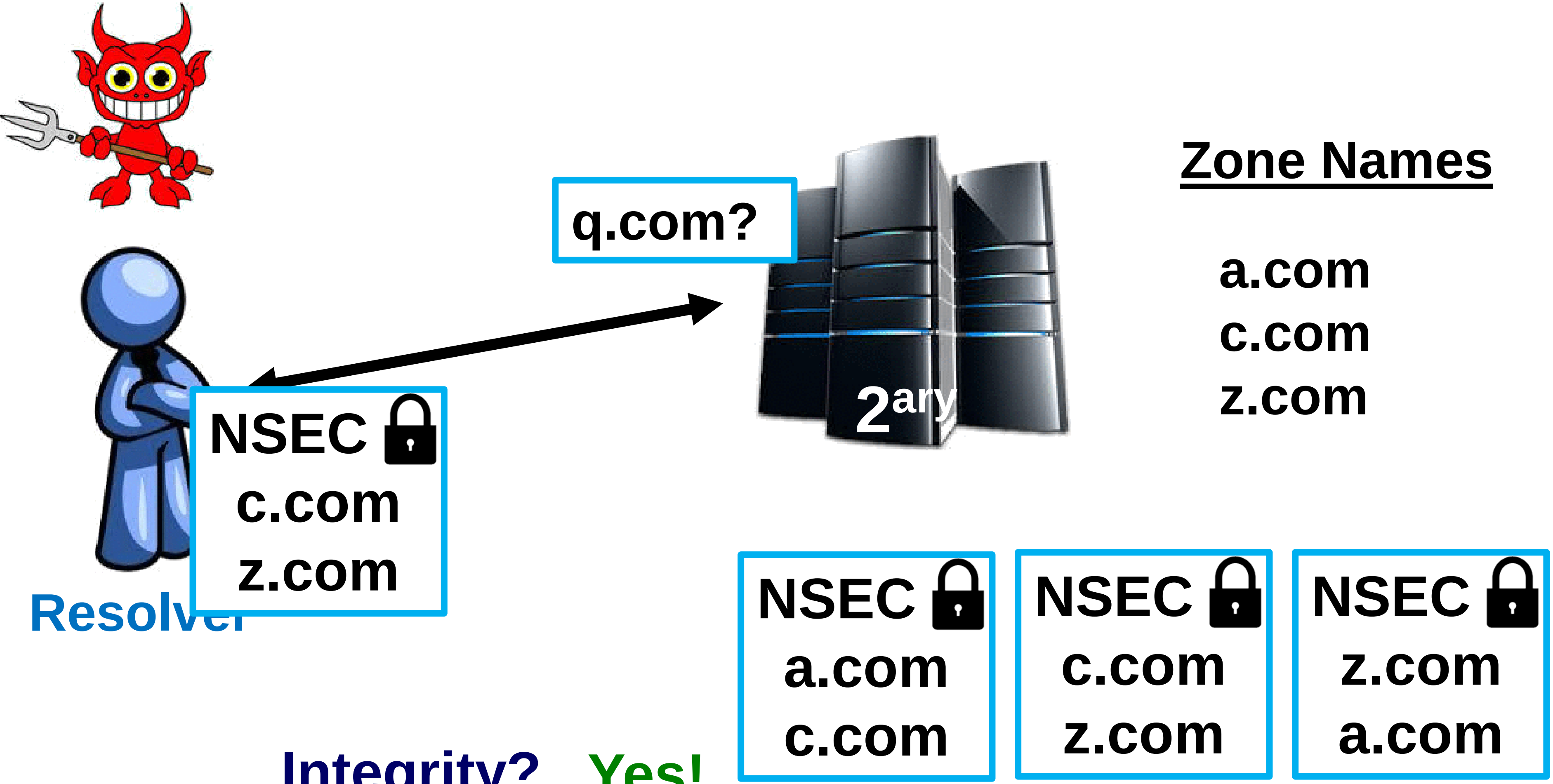
a.com
c.com
z.com

NSEC 🔒	NSEC 🔒	NSEC 🔒
a.com c.com	c.com z.com	z.com a.com

Integrity? Yes!

Privacy?

RFC 4034 – NSEC



q.com?

NSEC
c.com
z.com

Resolver

2ary

Zone Names

a.com
c.com
z.com

NSEC
a.com
c.com

NSEC
c.com
z.com

NSEC
z.com
a.com

Integrity? Yes!

Privacy? No! Can enumerate over the names

Zone enumeration is an issue

Zone enumeration is an issue

- Can expose private device names in the network

Zone enumeration is an issue

- Can expose private device names in the network
- Can be a source for probable email addresses for spam

Zone enumeration is an issue

- Can expose private device names in the network

- Can be a source for probable email addresses for spam

- Can be used to reveal information that domain registries are **legally obliged to protect**
  (e.g., EU-registries due to European Data Privacy Directive)

Zone enumeration is an issue

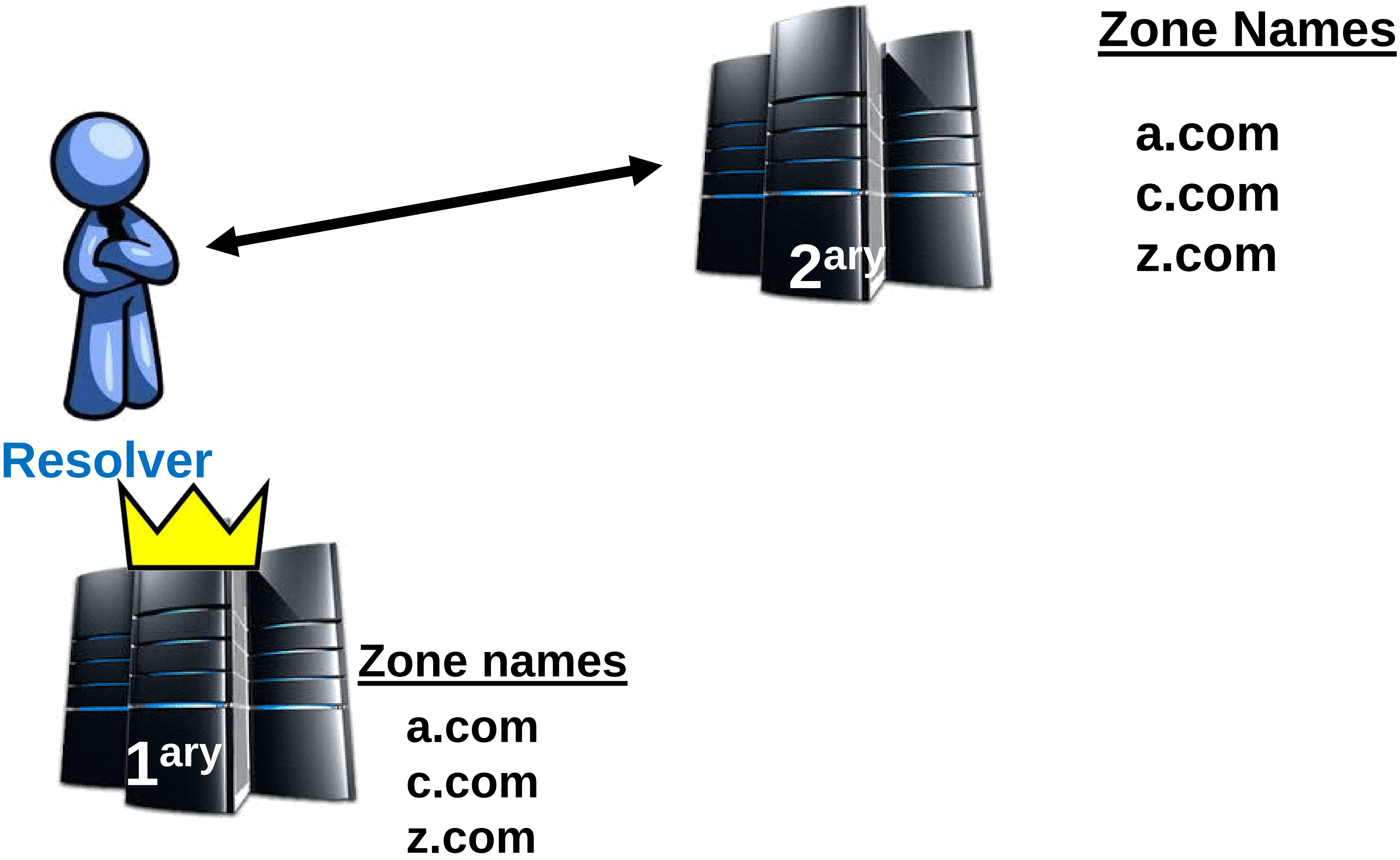
- Can expose private device names in the network

- Can be a source for probable email addresses for spam

- Can be used to reveal information that domain registries are **legally obliged to protect**
  (e.g., EU-registries due to European Data Privacy Directive)

- Formalized in **RFC 5155**, as a requirement for DNSSEC, which introduces **NSEC3**

RFC 5155 – NSEC3



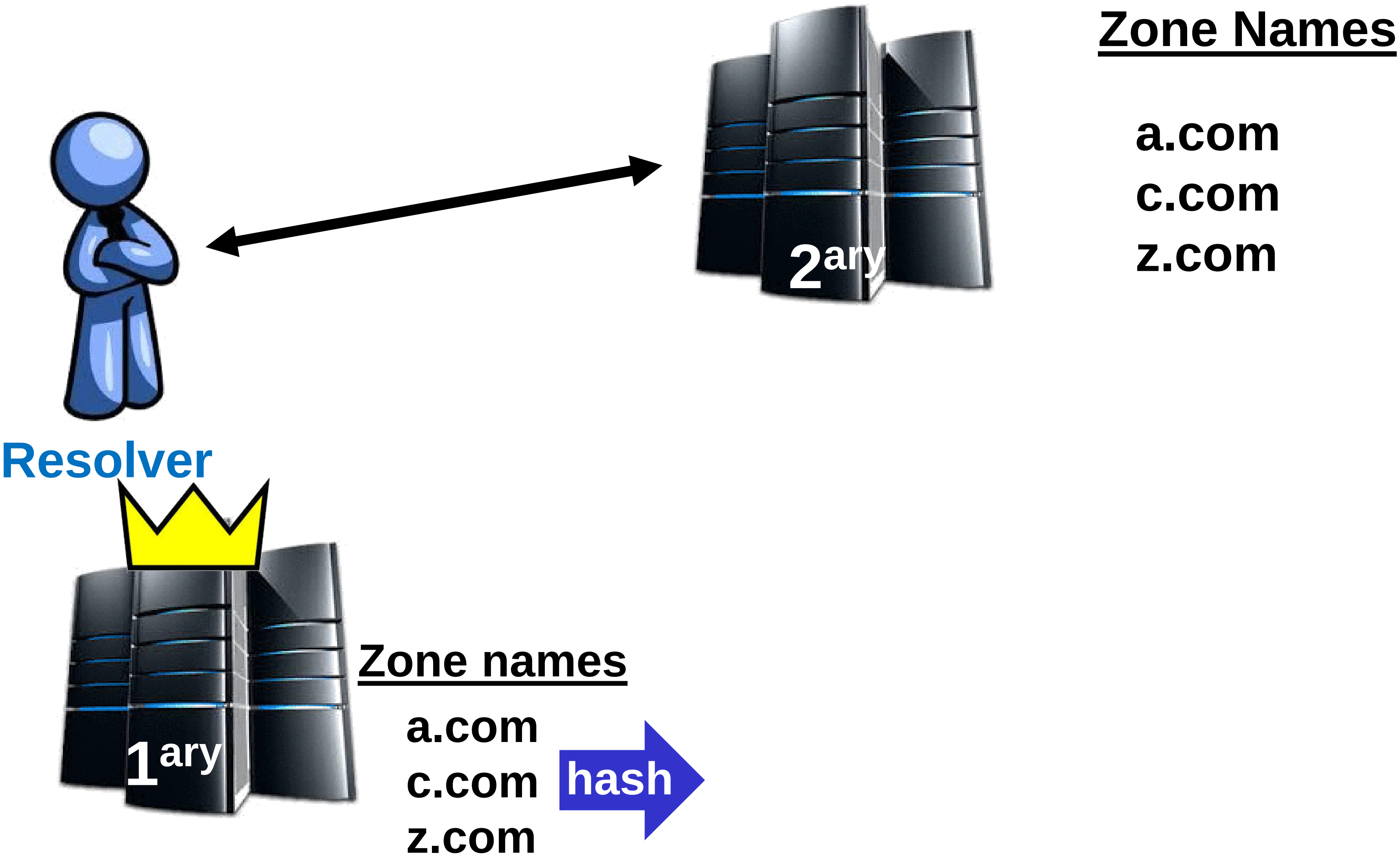
Zone Names

a.com
c.com
z.com

Zone names

a.com
c.com
z.com

RFC 5155 – NSEC3



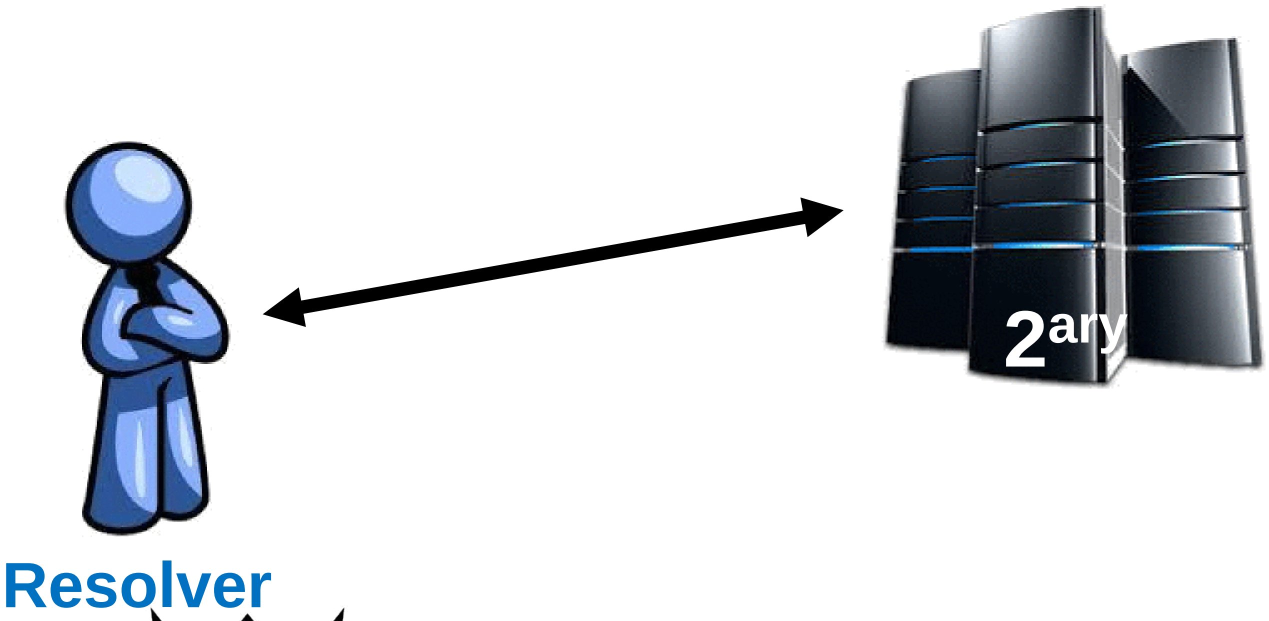
Zone Names

a.com
c.com
z.com

Zone names

a.com
c.com
z.com

RFC 5155 – NSEC3

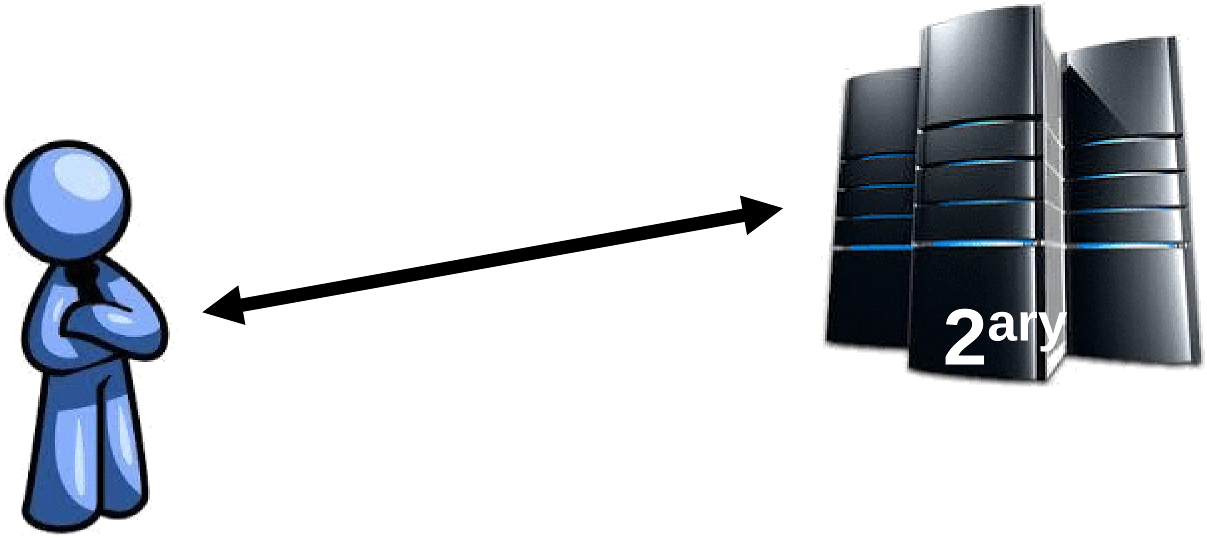


Zone Names

a.com
c.com
z.com

Zone names		**Zone hashes**
a.com		H(a.com)=a1bb5
c.com	hash →	H(c.com)=23ced
z.com		H(z.com)=dde45

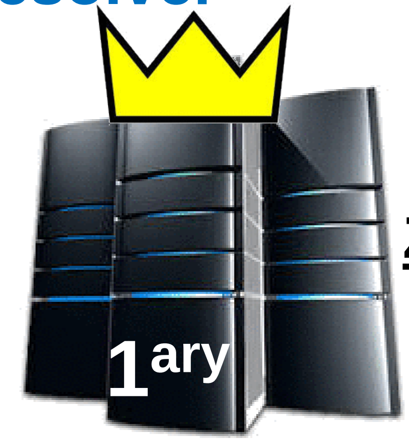
RFC 5155 – NSEC3



Resolver

Zone Names

a.com
c.com
z.com



Zone names

a.com
c.com
z.com

hash

Zone hashes

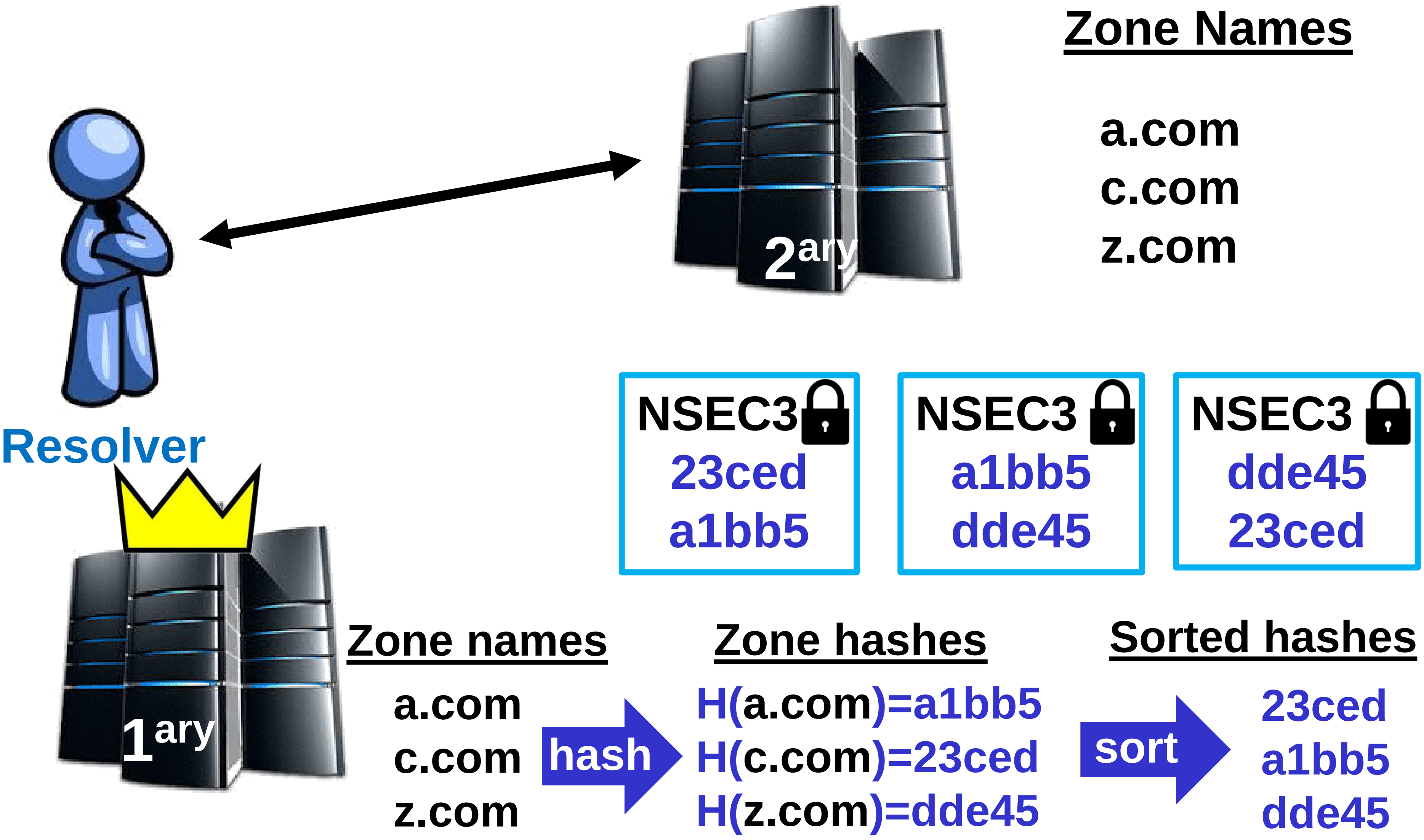
H(a.com)=a1bb5
H(c.com)=23ced
H(z.com)=dde45

sort

Sorted hashes

23ced
a1bb5
dde45

RFC 5155 – NSEC3



Zone Names

a.com
c.com
z.com

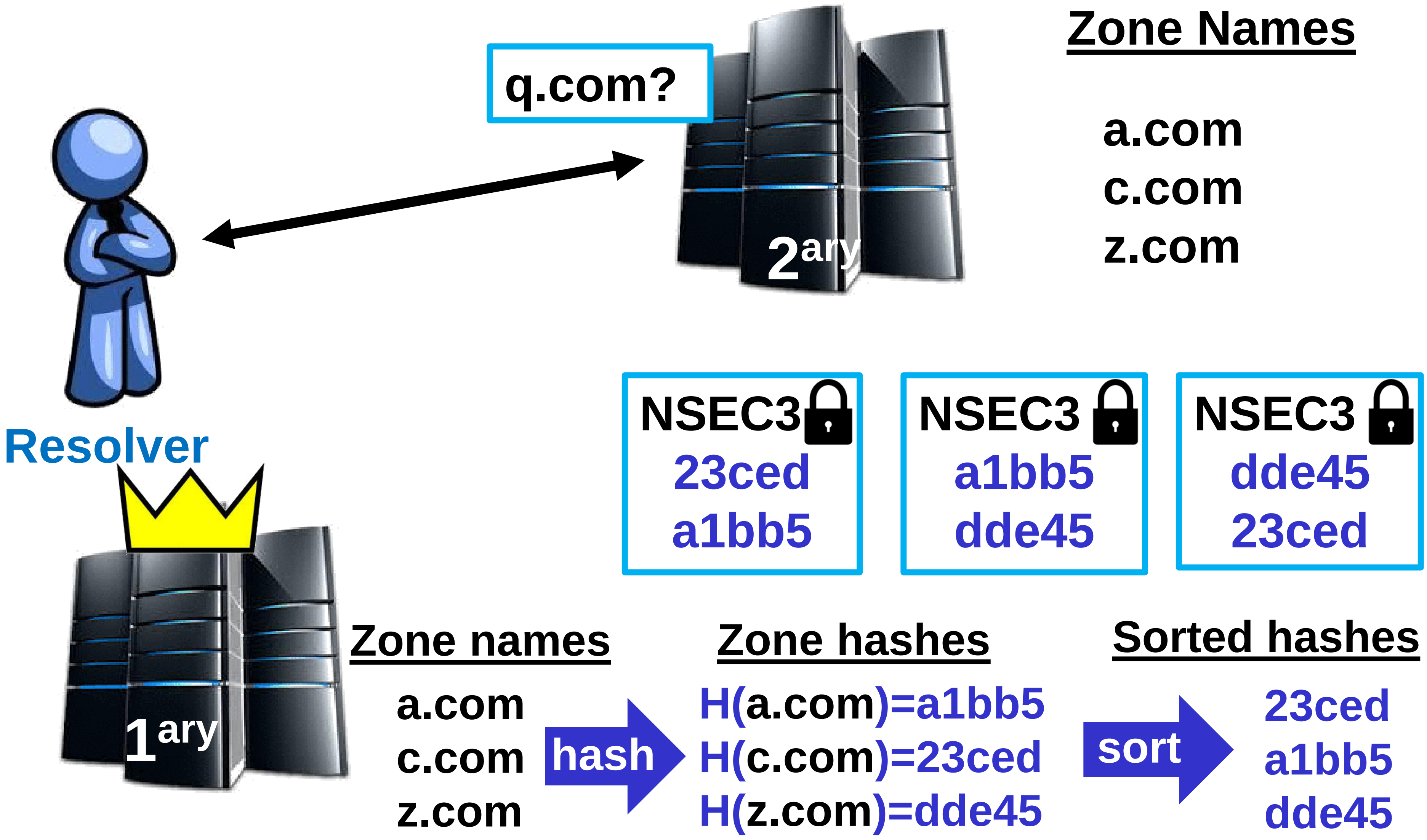
NSEC3 🔒
23ced
a1bb5

NSEC3 🔒
a1bb5
dde45

NSEC3 🔒
dde45
23ced

Zone names	Zone hashes	Sorted hashes
a.com	H(a.com)=a1bb5	23ced
c.com	H(c.com)=23ced	a1bb5
z.com	H(z.com)=dde45	dde45

RFC 5155 – NSEC3



q.com?

2^{ary}

Zone Names

a.com
c.com
z.com

Resolver

NSEC3
23ced
a1bb5

NSEC3
a1bb5
dde45

NSEC3
dde45
23ced

1^{ary}

Zone names

a.com
c.com
z.com

hash

Zone hashes

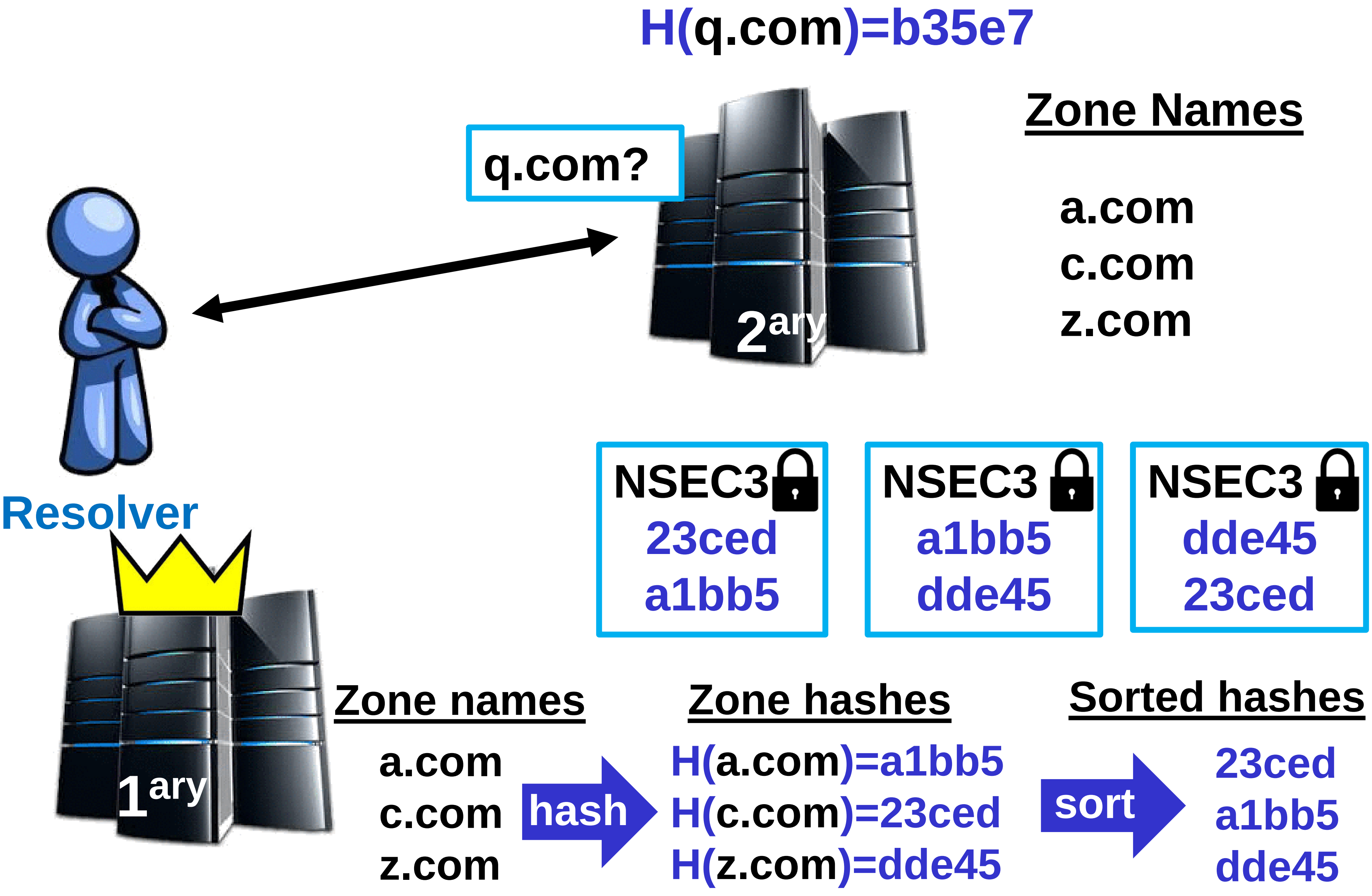
H(a.com)=a1bb5
H(c.com)=23ced
H(z.com)=dde45

sort

Sorted hashes

23ced
a1bb5
dde45

RFC 5155 – NSEC3



H(q.com)=b35e7

q.com?

2^{ary}

Zone Names

a.com
c.com
z.com

Resolver

NSEC3 🔒
23ced
a1bb5

NSEC3 🔒
a1bb5
dde45

NSEC3 🔒
dde45
23ced

1^{ary}

Zone names

a.com
c.com
z.com

hash

Zone hashes

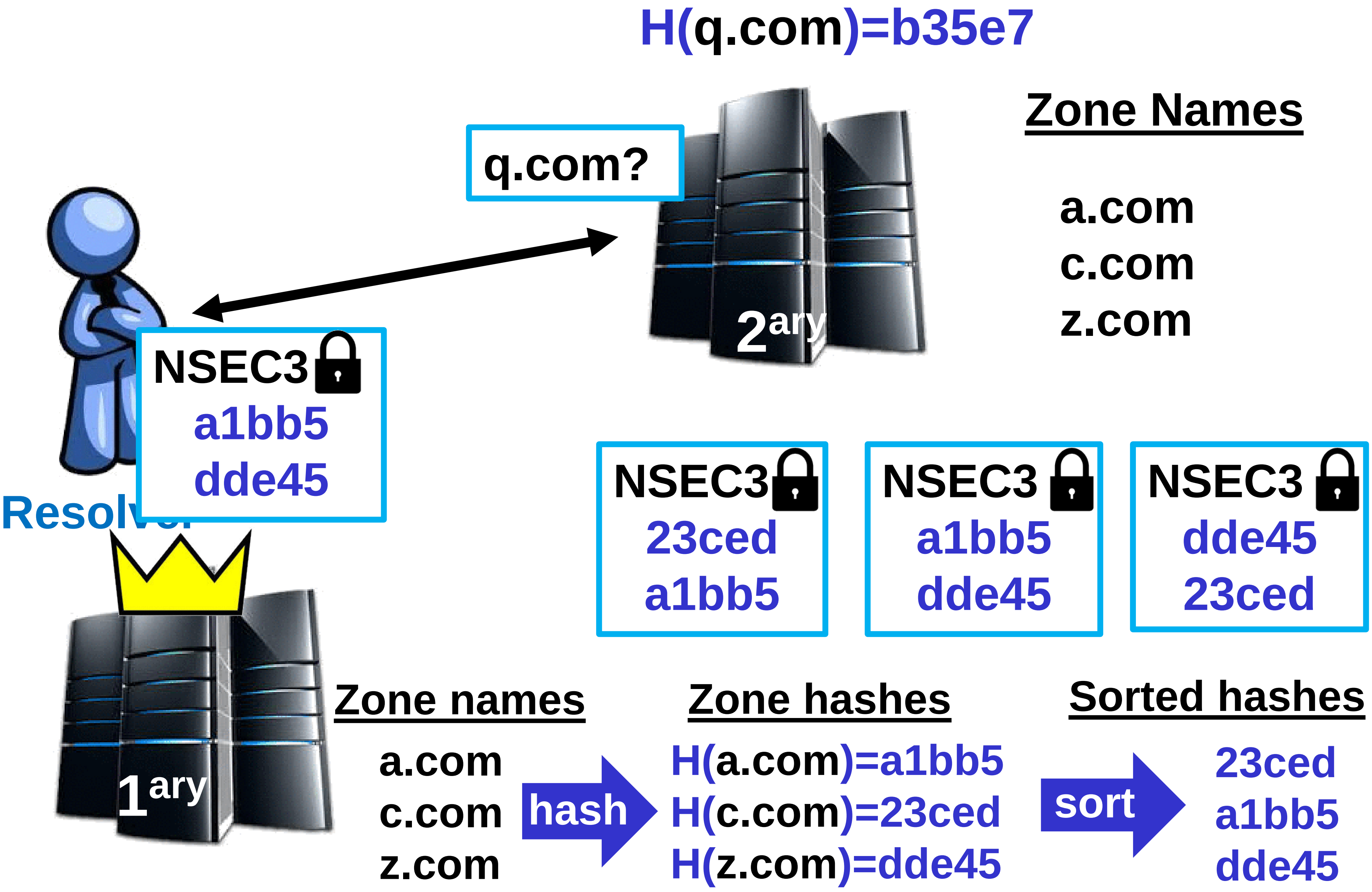
H(a.com)=a1bb5
H(c.com)=23ced
H(z.com)=dde45

sort

Sorted hashes

23ced
a1bb5
dde45

RFC 5155 – NSEC3



H(q.com)=b35e7

q.com?

Zone Names

a.com
c.com
z.com

NSEC3
a1bb5
dde45

Resolver

2ary

1ary

NSEC3
23ced
a1bb5

NSEC3
a1bb5
dde45

NSEC3
dde45
23ced

Zone names

a.com
c.com
z.com

hash

Zone hashes

H(a.com)=a1bb5
H(c.com)=23ced
H(z.com)=dde45

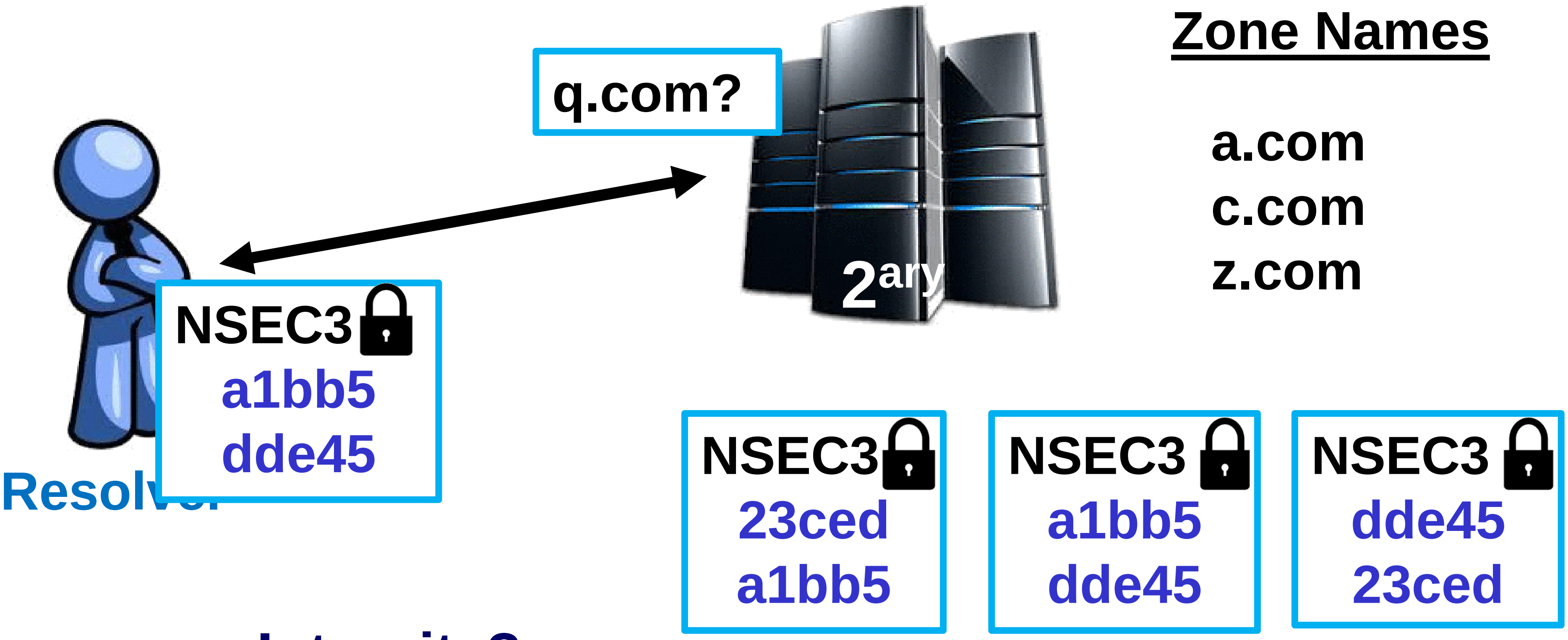
sort

Sorted hashes

23ced
a1bb5
dde45

RFC 5155 – NSEC3

H(q.com)=b35e7



q.com?

NSEC3
a1bb5
dde45

Resolver

2^{ary}

Zone Names

a.com
c.com
z.com

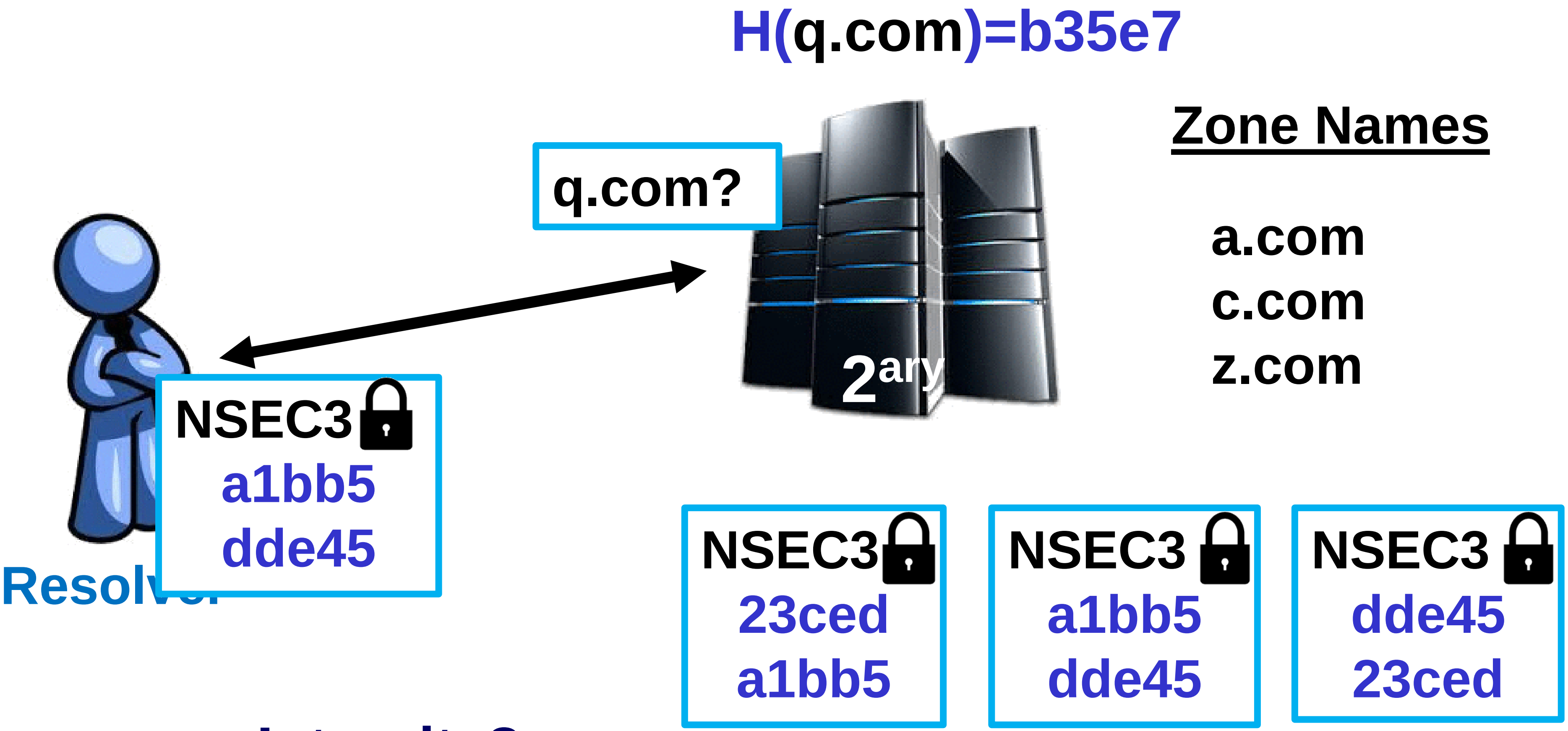
NSEC3
23ced
a1bb5

NSEC3
a1bb5
dde45

NSEC3
dde45
23ced

Integrity?

RFC 5155 – NSEC3



H(q.com)=b35e7

q.com?

Zone Names

a.com
c.com
z.com

2^{ary}

NSEC3
a1bb5
dde45

Resolver

NSEC3
23ced
a1bb5

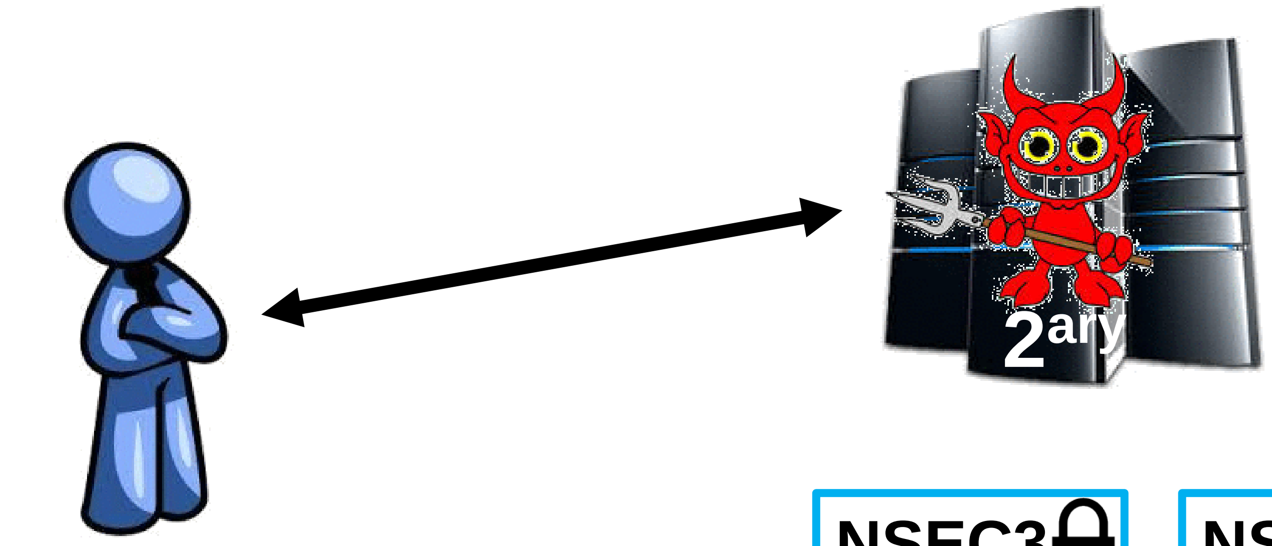
NSEC3
a1bb5
dde45

NSEC3
dde45
23ced

Integrity?

Privacy?

RFC 5155 – NSEC3



Resolver

Zone Names

a.com
c.com
z.com

NSEC3 🔒
23ced
a1bb5

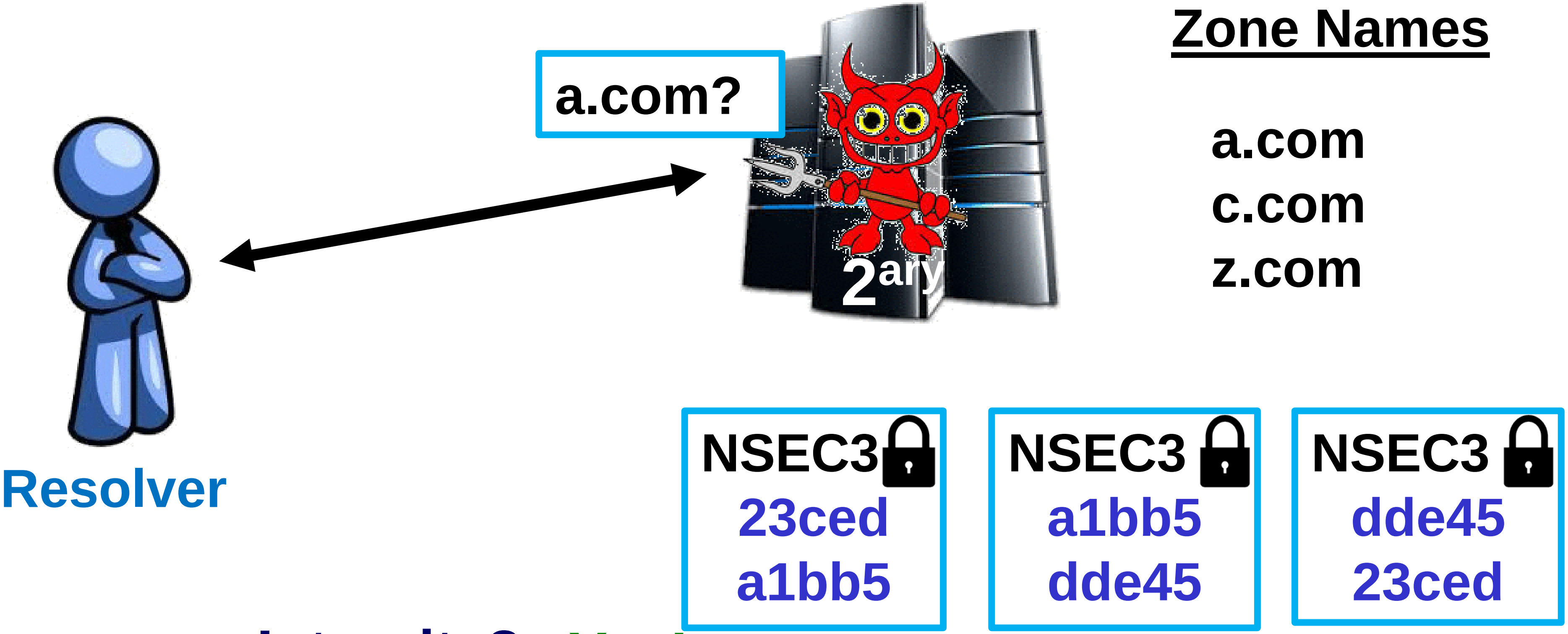
NSEC3 🔒
a1bb5
dde45

NSEC3 🔒
dde45
23ced

Integrity? Yes!

Privacy?

RFC 5155 – NSEC3



Zone Names

a.com
c.com
z.com

NSEC3 🔒
23ced
a1bb5

NSEC3 🔒
a1bb5
dde45

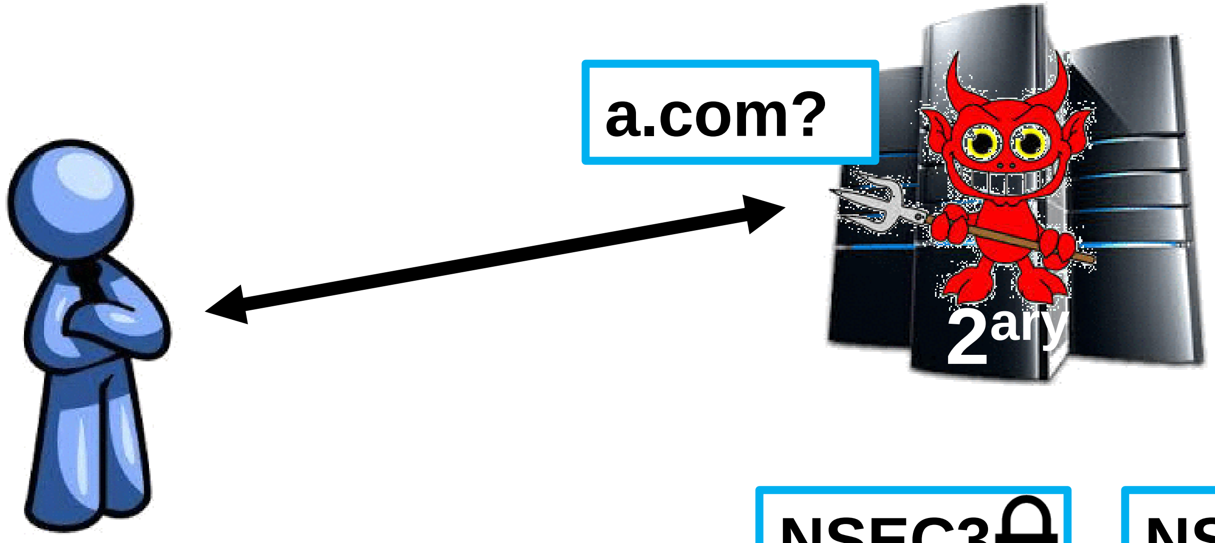
NSEC3 🔒
dde45
23ced

Integrity? **Yes!**

Privacy?

RFC 5155 – NSEC3

H(a.com)=a1bb5



Resolver

Zone Names

a.com
c.com
z.com

NSEC3 🔒
23ced
a1bb5

NSEC3 🔒
a1bb5
dde45

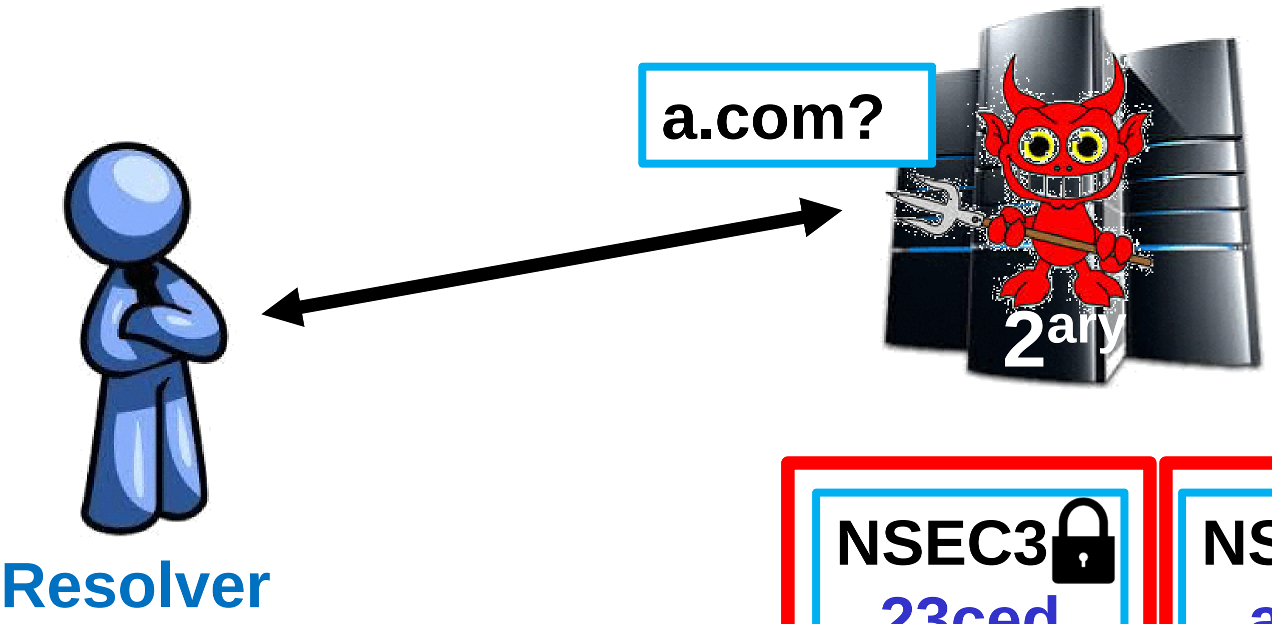
NSEC3 🔒
dde45
23ced

Integrity? Yes!

Privacy?

RFC 5155 – NSEC3

H(a.com)=a1bb5



Zone Names

a.com
c.com
z.com

NSEC3🔒
23ced
a1bb5

NSEC3🔒
a1bb5
dde45

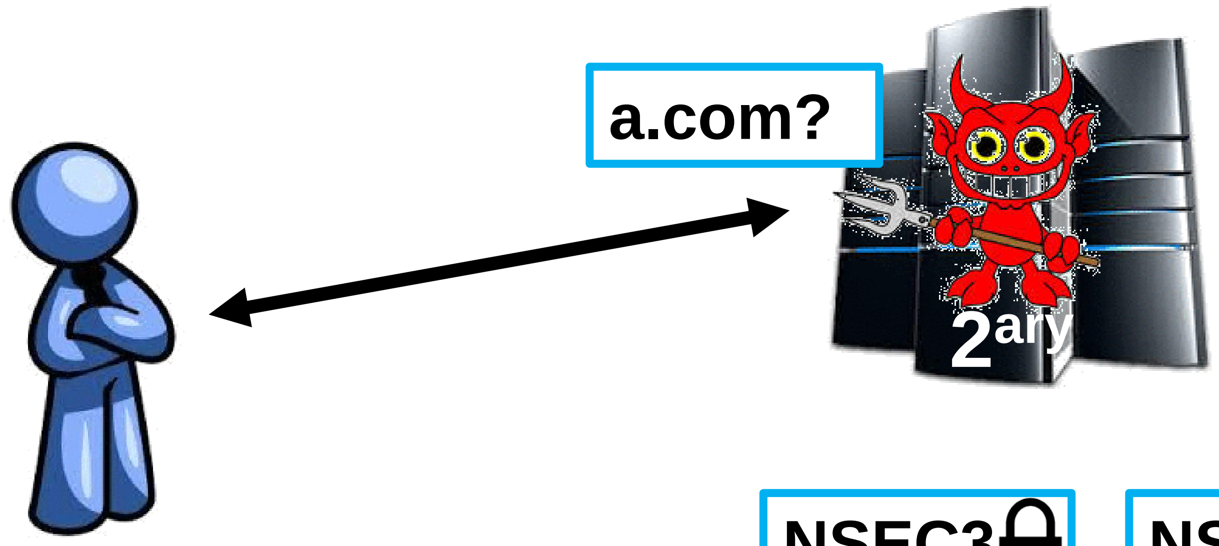
NSEC3🔒
dde45
23ced

Integrity? Yes!

Privacy?

RFC 5155 – NSEC3

H(a.com)=a1bb5



a.com?

Resolver

Zone Names

a.com
c.com
z.com

NSEC3
23ced
a1bb5

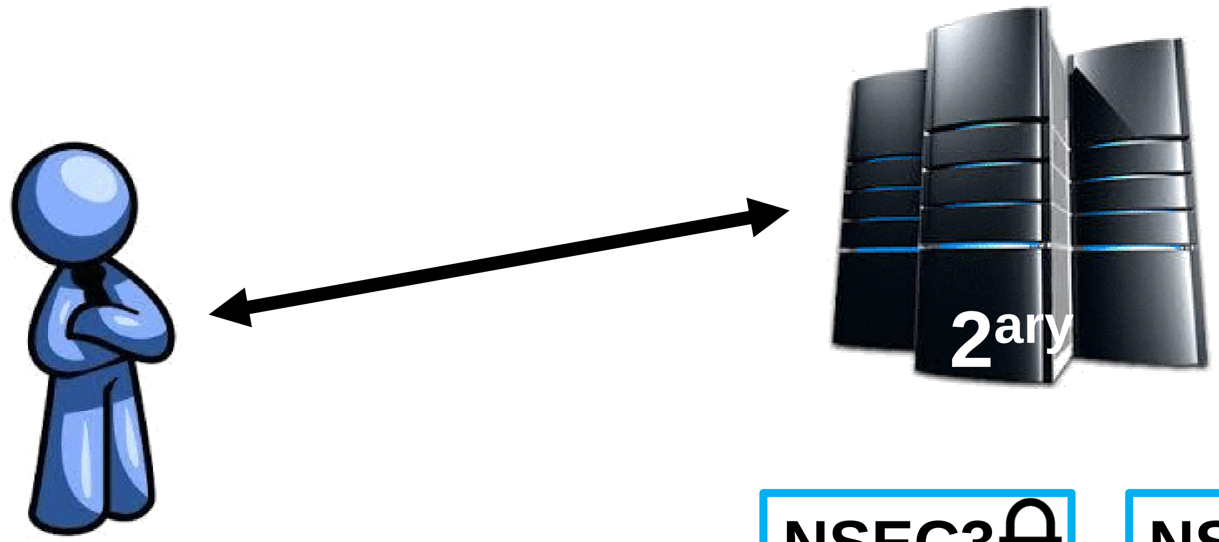
NSEC3
a1bb5
dde45

NSEC3
dde45
23ced

Integrity? Yes!

Privacy?

RFC 5155 – NSEC3



Resolver

Zone Names

a.com
c.com
z.com

NSEC3 🔒
23ced
a1bb5

NSEC3 🔒
a1bb5
dde45

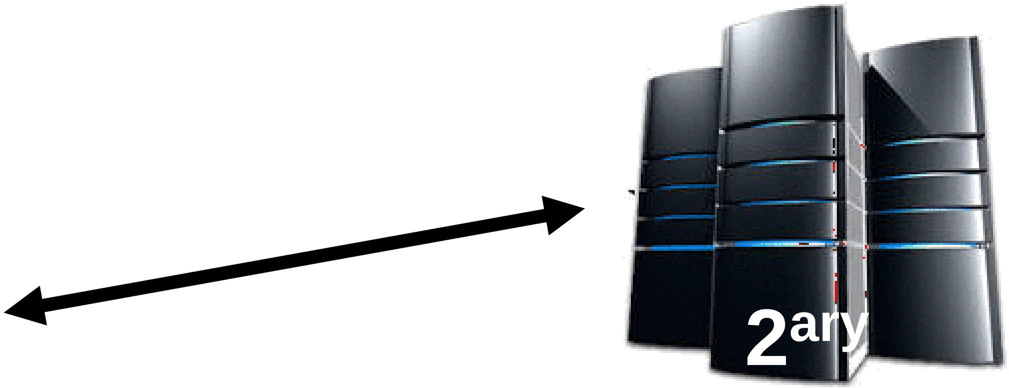
NSEC3 🔒
dde45
23ced

Integrity? Yes!

Privacy? Still no

Zone enumeration in NSEC3

Resolver



Zone Names

a.com
c.com
z.com

NSEC3
23ced
a1bb5

NSEC3
a1bb5
dde45

NSEC3
dde45
23ced

Zone enumeration in NSEC3

Random queries

Resolver

Zone Names

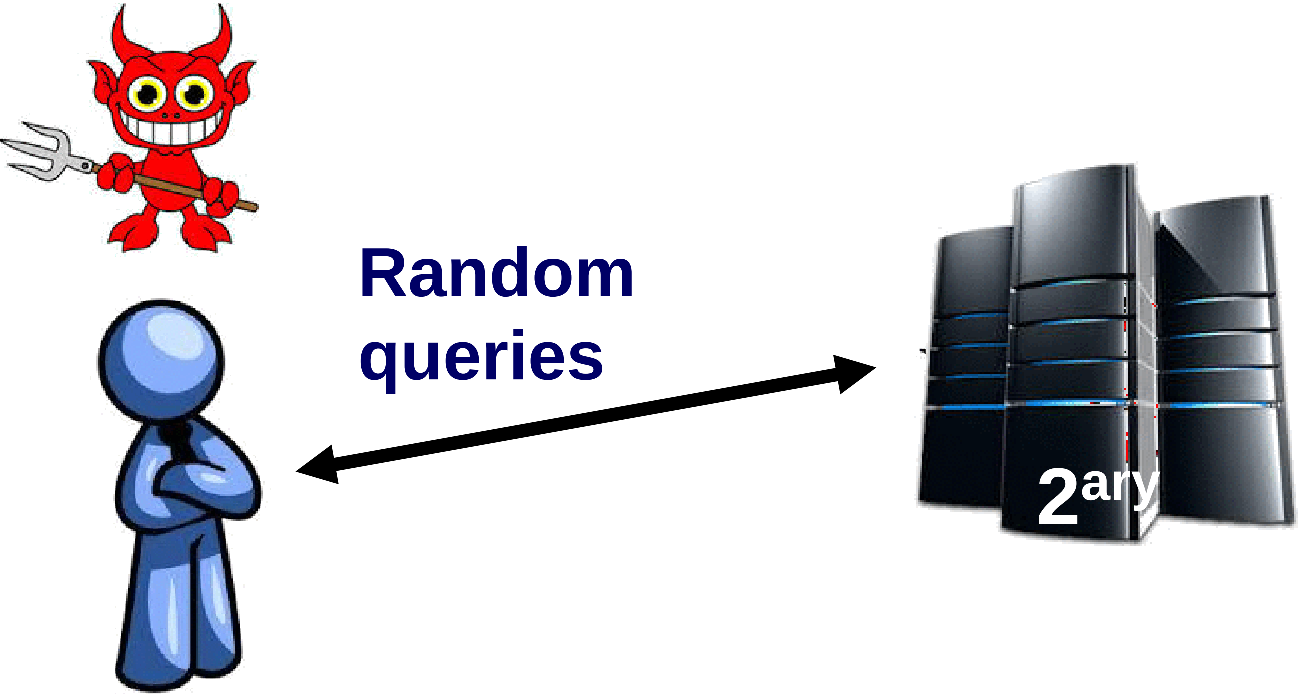
a.com
c.com
z.com

NSEC3
23ced
a1bb5

NSEC3
a1bb5
dde45

NSEC3
dde45
23ced

Zone enumeration in NSEC3



Resolver

Zone Names

a.com
c.com
z.com

NSEC3🔒
23ced
a1bb5

NSEC3🔒
a1bb5
dde45

NSEC3🔒
dde45
23ced

Zone enumeration in NSEC3

Random queries

Zone Names

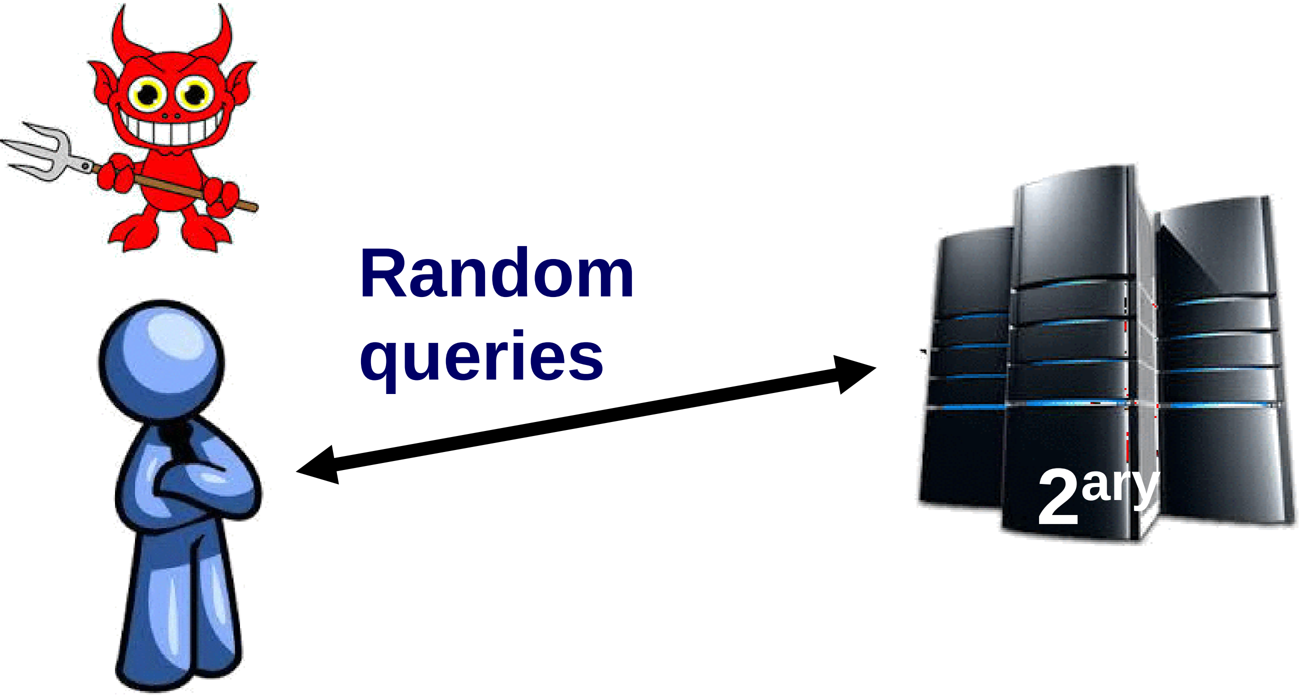
a.com
c.com
z.com

Resolver

Learned hashes

23ced
a1bb5
dde45

Zone enumeration in NSEC3



Resolver

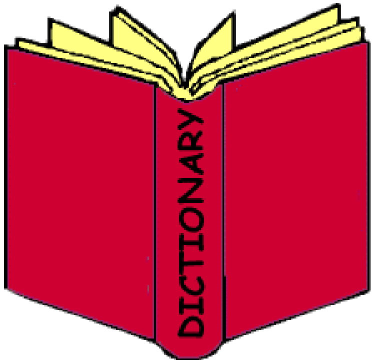
Zone Names

a.com
c.com
z.com

Learned hashes

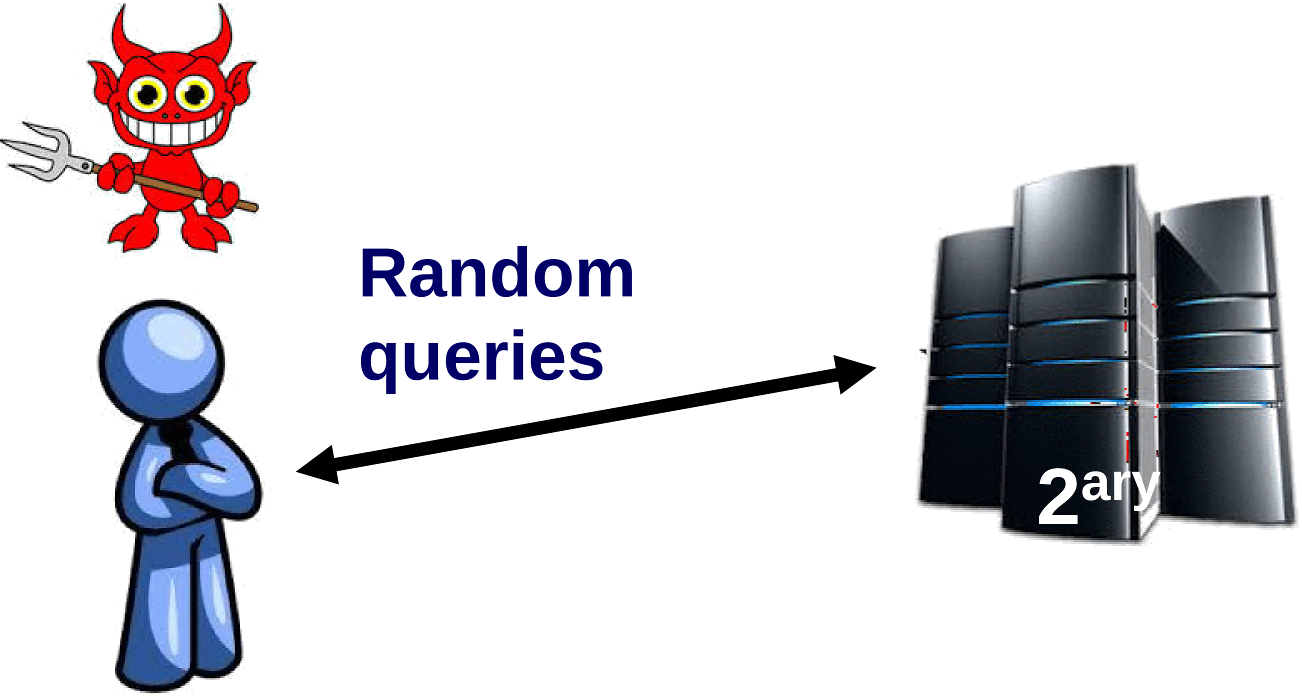
23ced
a1bb5
dde45

Make a dictionary of plausible names



a.com
b.com
c.com
...
z.com

Zone enumeration in NSEC3



Random queries

Zone Names

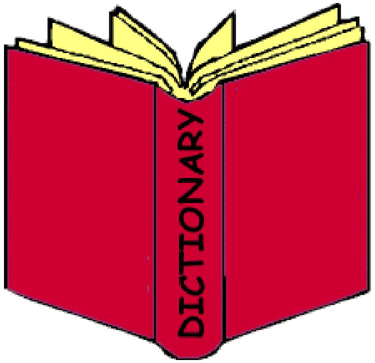
a.com
c.com
z.com

Resolver

Learned hashes

23ced
a1bb5
dde45

Make a dictionary of plausible names

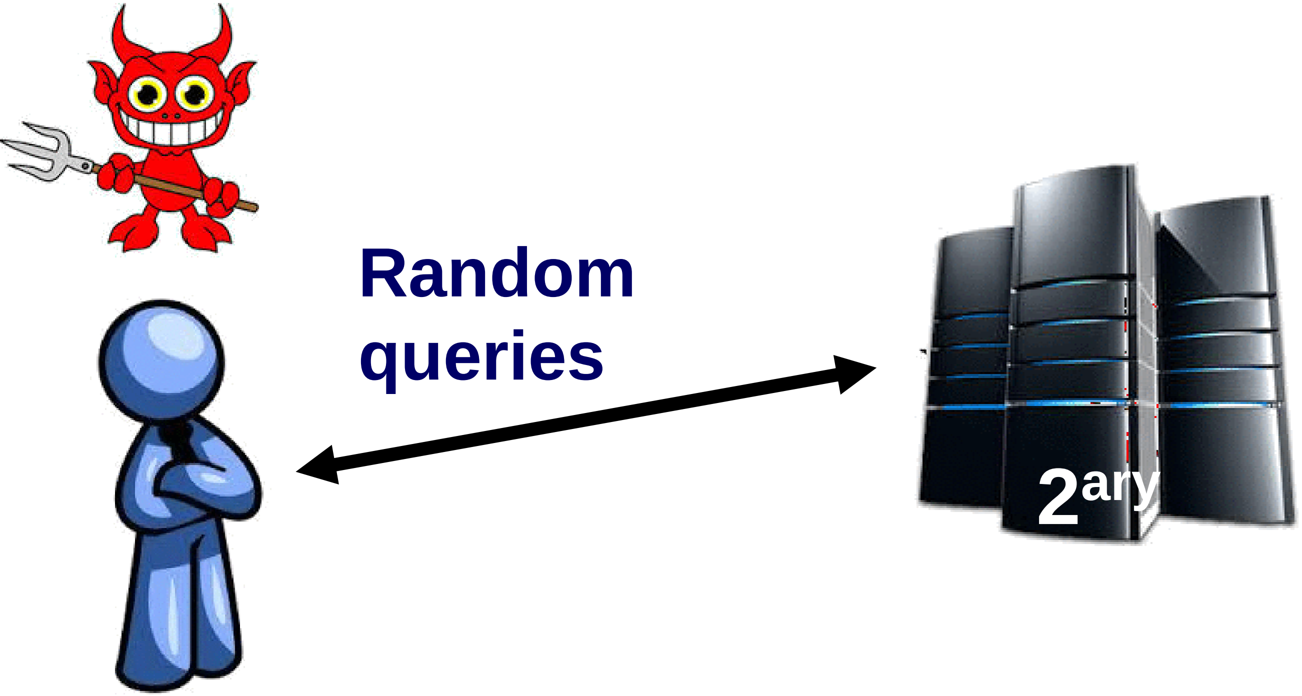


a.com
b.com
c.com
...
z.com

Hash dictionary to find matches

H(a.com)=a1bb5
H(b.com)=a1bb5
H(c.com)=23ced
H(z.com)=dde45

Zone enumeration in NSEC3



Random queries

Zone Names

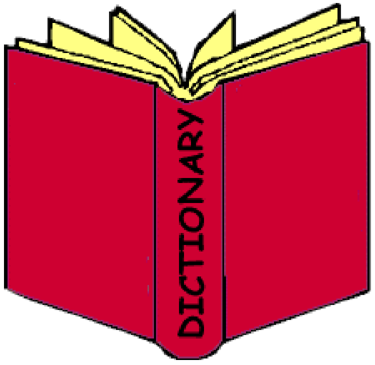
a.com
c.com
z.com

Resolver

Learned hashes

23ced
a1bb5
dde45

Make a dictionary of plausible names

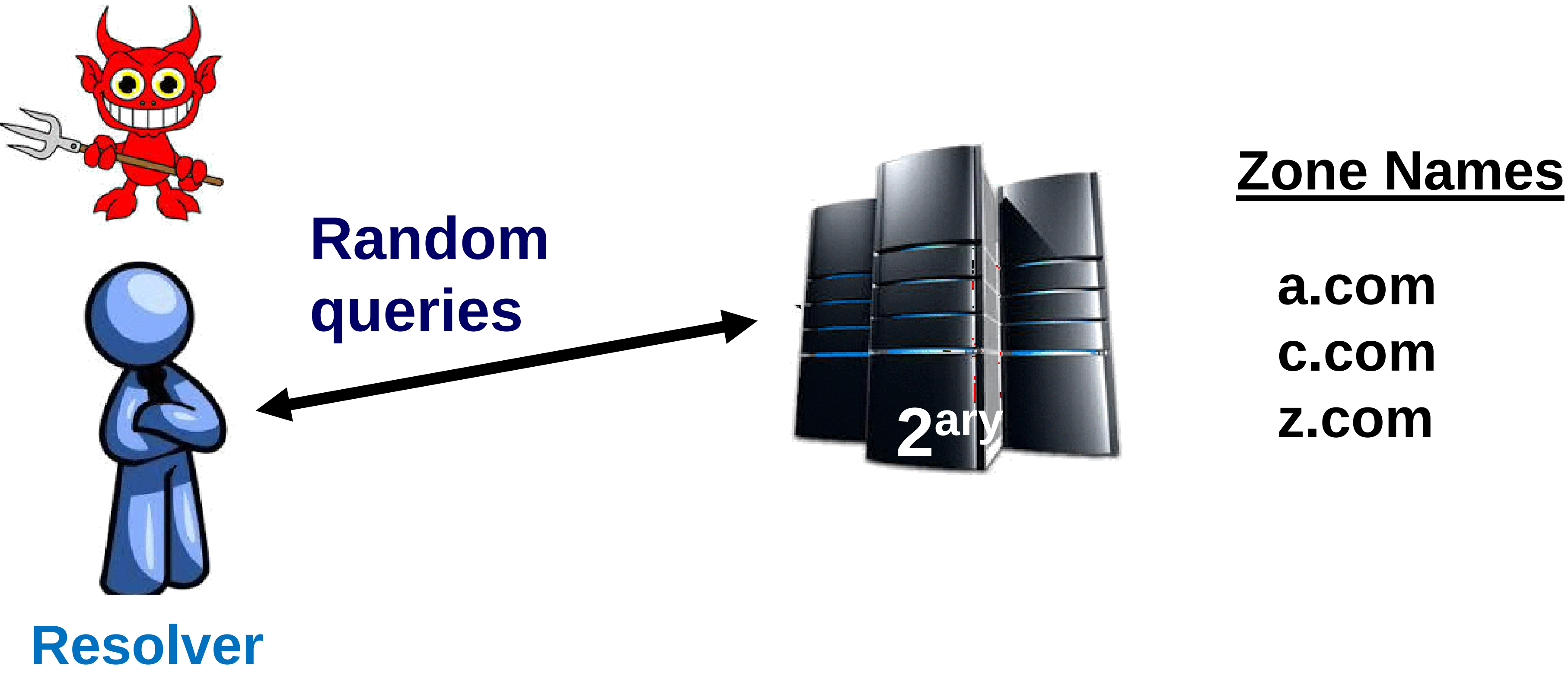


a.com
b.com
c.com
...
z.com

Hash dictionary to find matches

H(a.com)=a1bb5
H(b.com)=a1bb5
H(c.com)=23ced
H(z.com)=dde45

Zone enumeration in NSEC3



Random queries

Zone Names

a.com
c.com
z.com

Resolver

NSEC3 zone enumeration has been demonstrated:

- [Wander, Schwittmann, Boelmann, Weis 2014] enumerated **64% of the .com** TLD in **under 5 days** using **one GPU**.
- In 2011, [Bernstein]'s nsec3walker guessed 2^{34} hashes/per day on a laptop.

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2^dry^ nameserver	No zone enumeration
DNS	✗	✗	✓

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2^dry^ nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2dry nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2dry nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

NSEC5 Desiderata

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

NSEC5 Desiderata

1. **Integrity** (even when the nameserver was compromised)

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2dry nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

NSEC5 Desiderata

1. **Integrity** (even when the nameserver was compromised)
2. Preventing **Zone enumeration**

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2^dry^ nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

NSEC5 Desiderata

1. **Integrity** (even when the nameserver was compromised)
2. Preventing **Zone enumeration**
3. **Efficiency** and **simplicity** (e.g. no “exotic” crypto)

The idea for constructing NSEC5

The idea for constructing NSEC5

Reason NSEC3 failed to prevent zone enumeration:

Resolvers can compute hashes offline

The idea for constructing NSEC5

Reason NSEC3 failed to prevent zone enumeration:

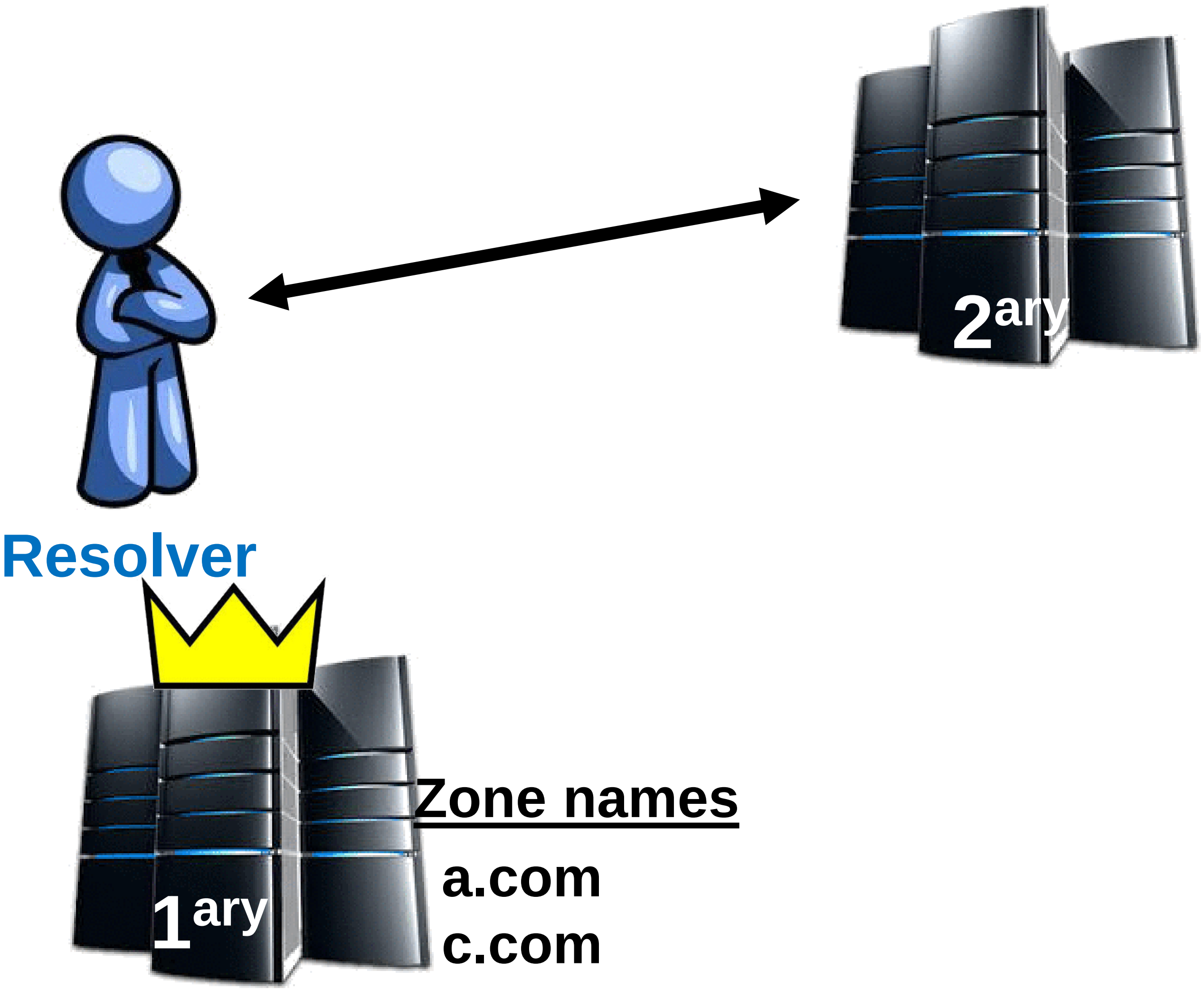
Resolvers can compute hashes offline

Solution:

add a **Secret NSEC5 Key** and a **Public NSEC5 Key**

required to compute and verify the hashes respectively

NSEC5 – Primary setup



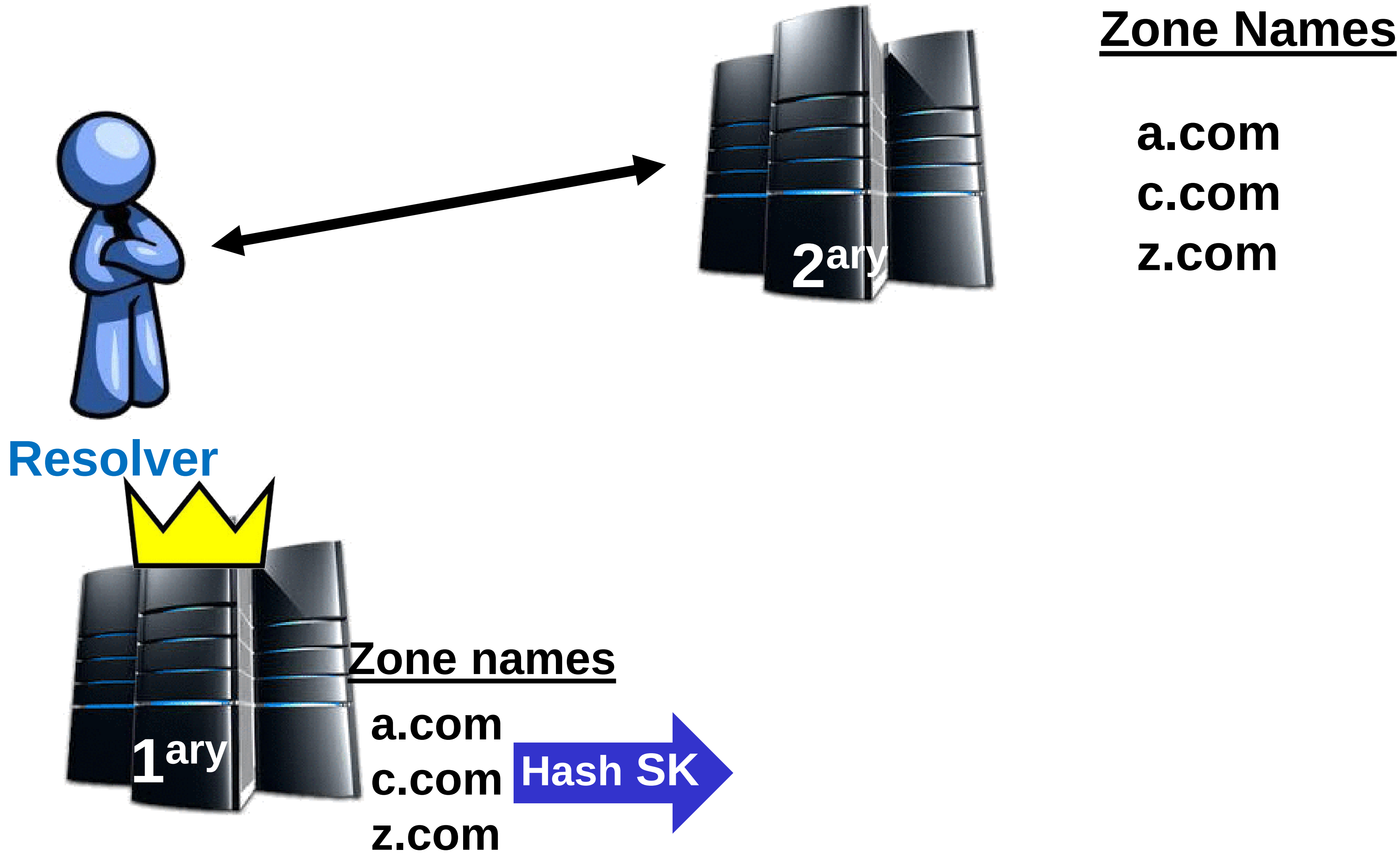
Zone Names

a.com
c.com
z.com

Zone names

a.com
c.com
z.com

NSEC5 – Primary setup



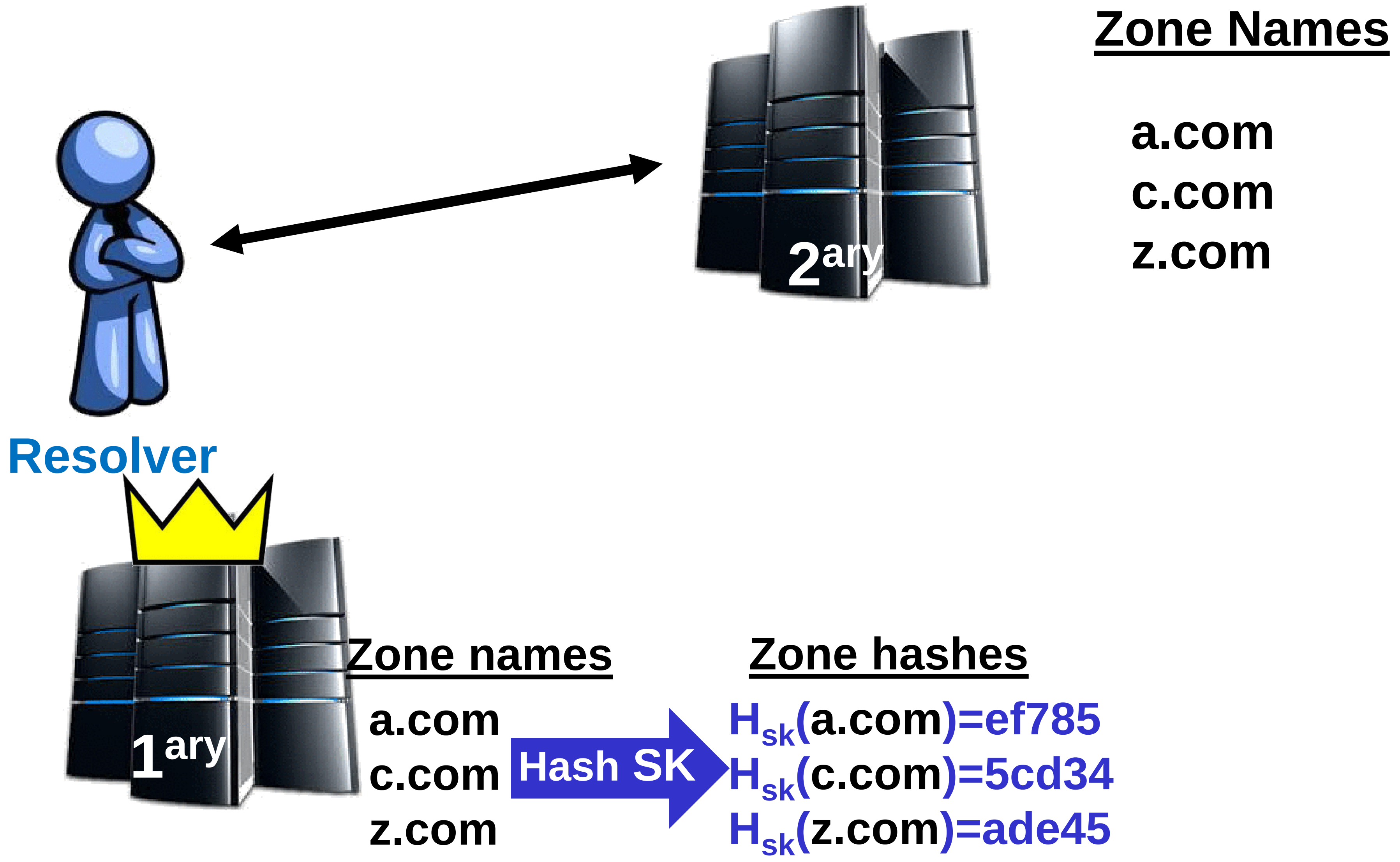
Zone Names

a.com
c.com
z.com

Zone names

a.com
c.com
z.com

NSEC5 – Primary setup



Resolver

2ary

Zone Names

a.com
c.com
z.com

1ary

Zone names

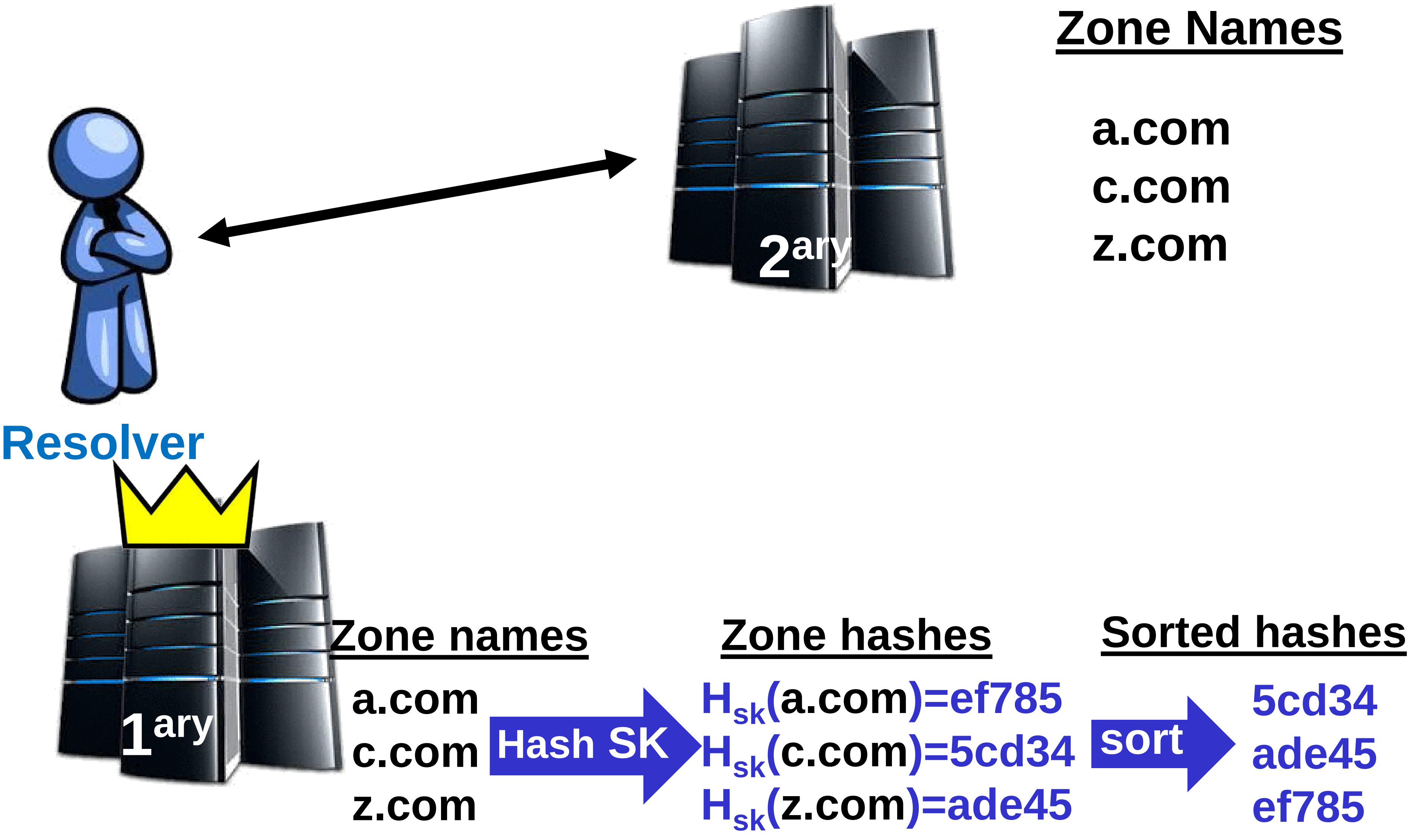
a.com
c.com
z.com

Hash SK

Zone hashes

H_{sk}(a.com)=ef785
H_{sk}(c.com)=5cd34
H_{sk}(z.com)=ade45

NSEC5 – Primary setup



Zone Names

a.com
c.com
z.com

Resolver

Zone names

a.com
c.com
z.com

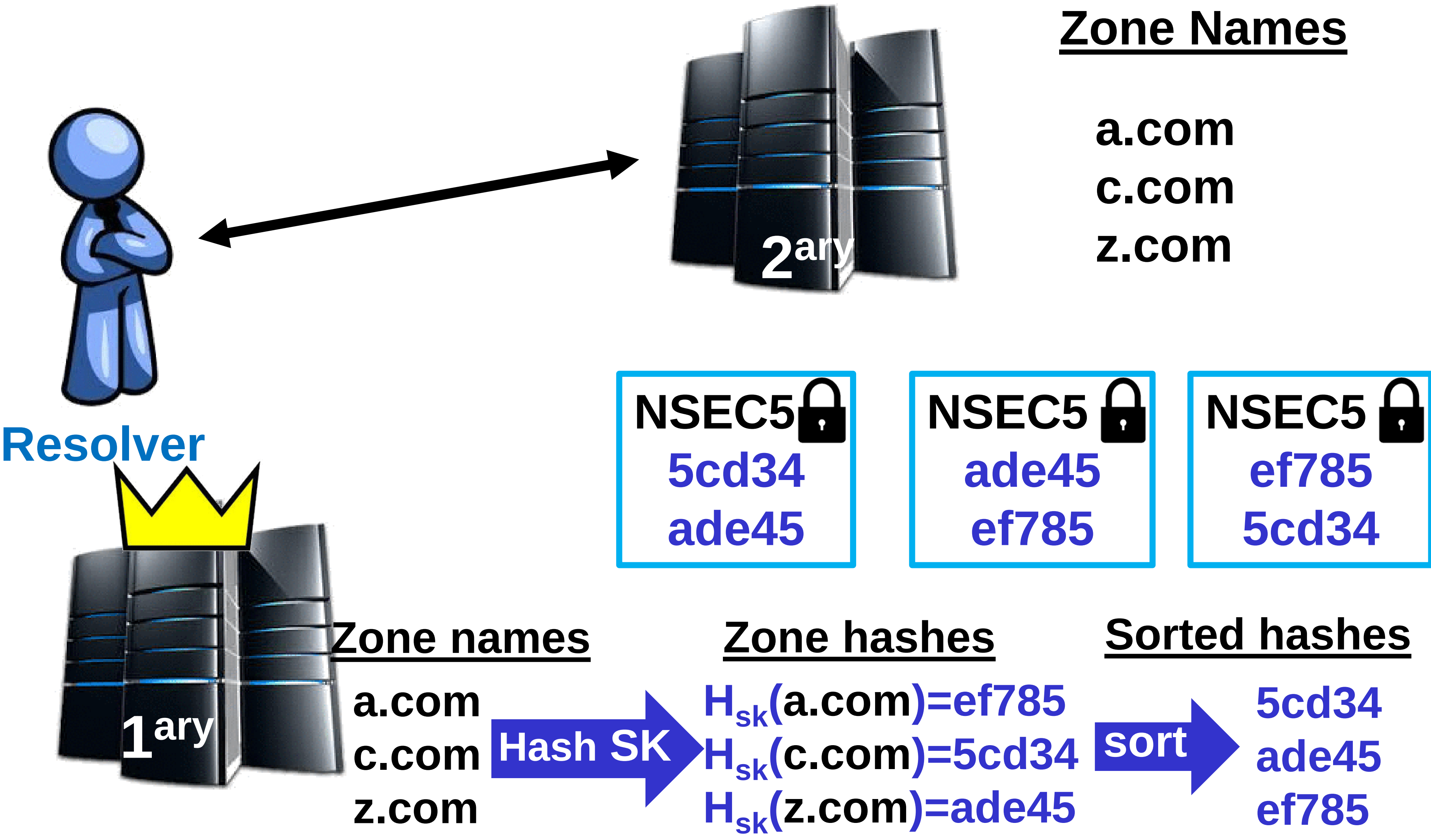
Zone hashes

H_{sk}(a.com)=ef785
H_{sk}(c.com)=5cd34
H_{sk}(z.com)=ade45

Sorted hashes

5cd34
ade45
ef785

NSEC5 – Primary setup



Zone Names

a.com
c.com
z.com

NSEC5	NSEC5	NSEC5
5cd34	ade45	ef785
ade45	ef785	5cd34

Zone names

a.com
c.com
z.com

Zone hashes

H_{sk}(a.com)=ef785
H_{sk}(c.com)=5cd34
H_{sk}(z.com)=ade45

Sorted hashes

5cd34
ade45
ef785

NSEC5 – Primary setup

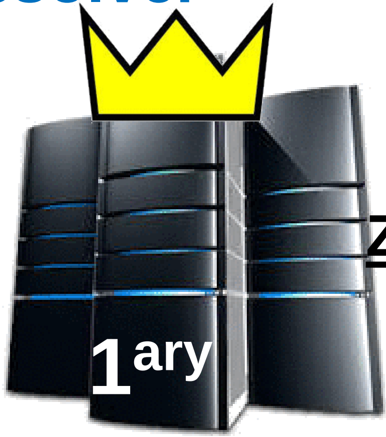
Resolver

Zone Names

a.com
c.com
z.com

Secret NSEC5 Key

NSEC5 🔒 5cd34 ade45	NSEC5 🔒 ade45 ef785	NSEC5 🔒 ef785 5cd34



Zone names

a.com
c.com
z.com

Hash SK

Zone hashes

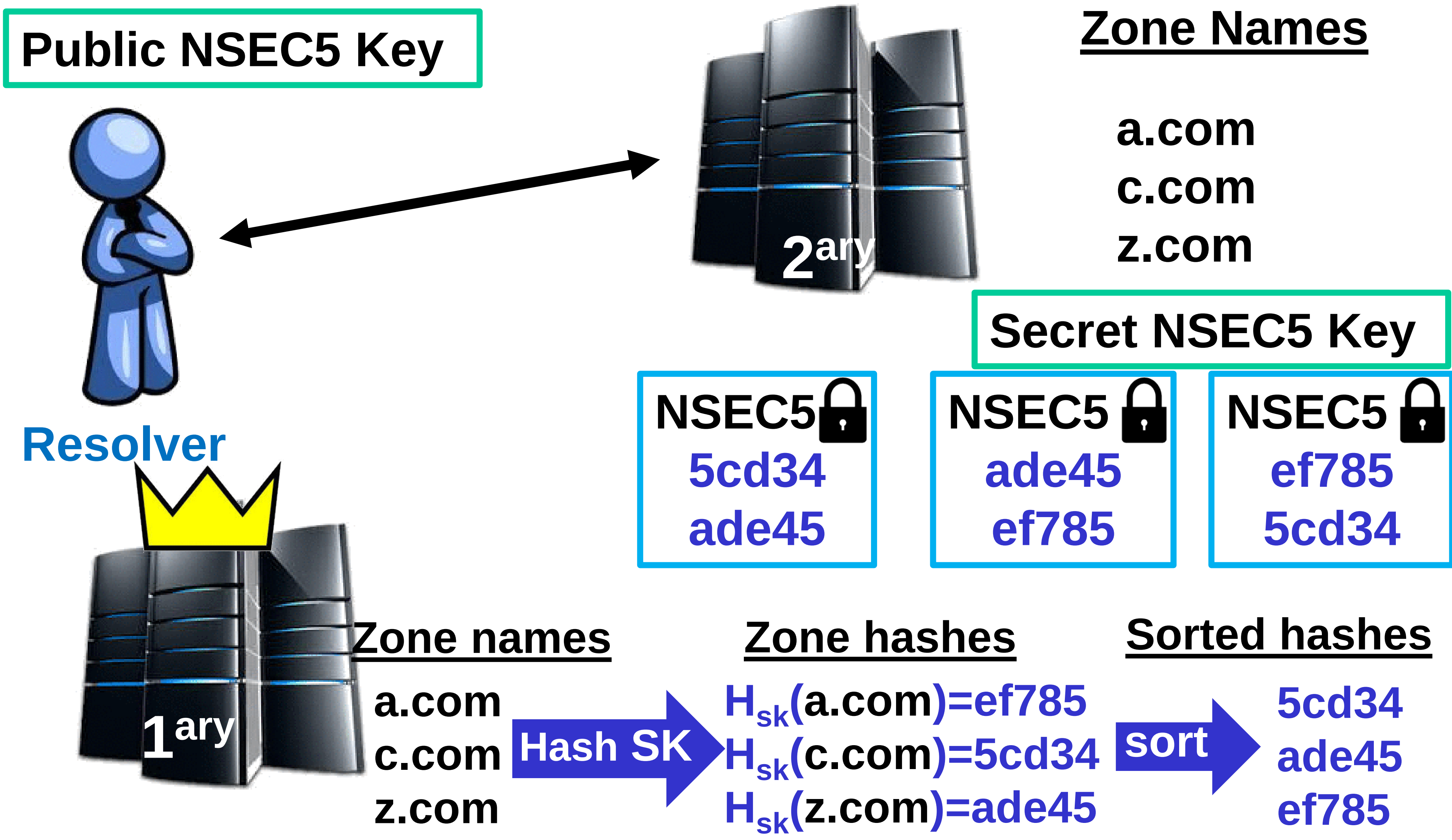
H_{sk}(a.com)=ef785
H_{sk}(c.com)=5cd34
H_{sk}(z.com)=ade45

sort

Sorted hashes

5cd34
ade45
ef785

NSEC5 – Primary setup



Public NSEC5 Key

Resolver

2^{ary}

Zone Names

a.com
c.com
z.com

Secret NSEC5 Key

NSEC5 🔒 5cd34 ade45	NSEC5 🔒 ade45 ef785	NSEC5 🔒 ef785 5cd34

1^{ary}

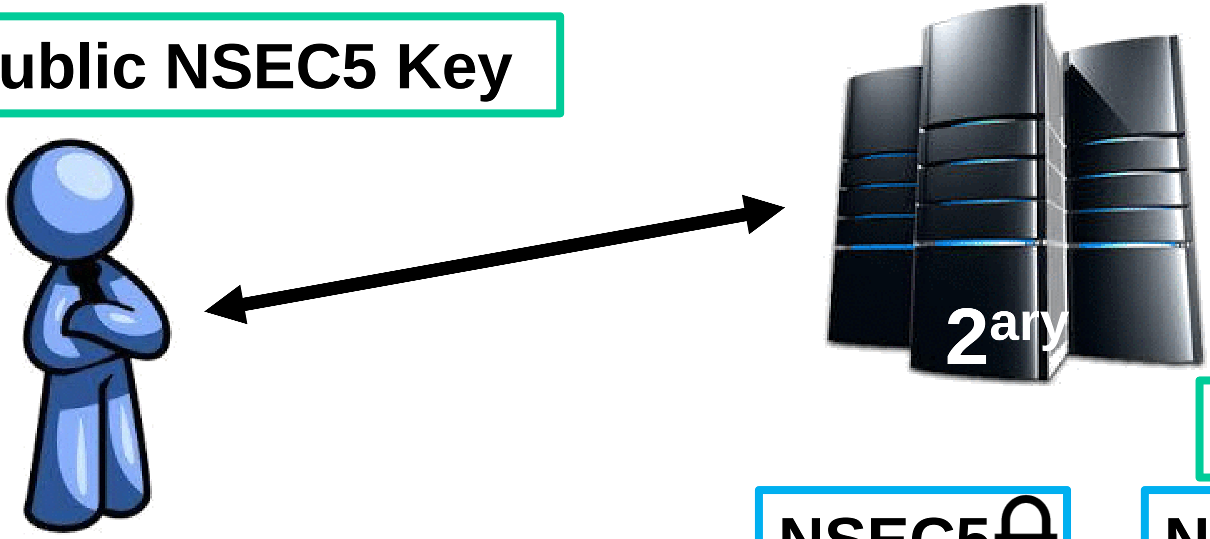
Hash SK

sort

Zone names	Zone hashes	Sorted hashes
a.com	H_{sk}(a.com)=ef785	5cd34
c.com	H_{sk}(c.com)=5cd34	ade45
z.com	H_{sk}(z.com)=ade45	ef785

NSEC5 in action

Public NSEC5 Key



Resolver

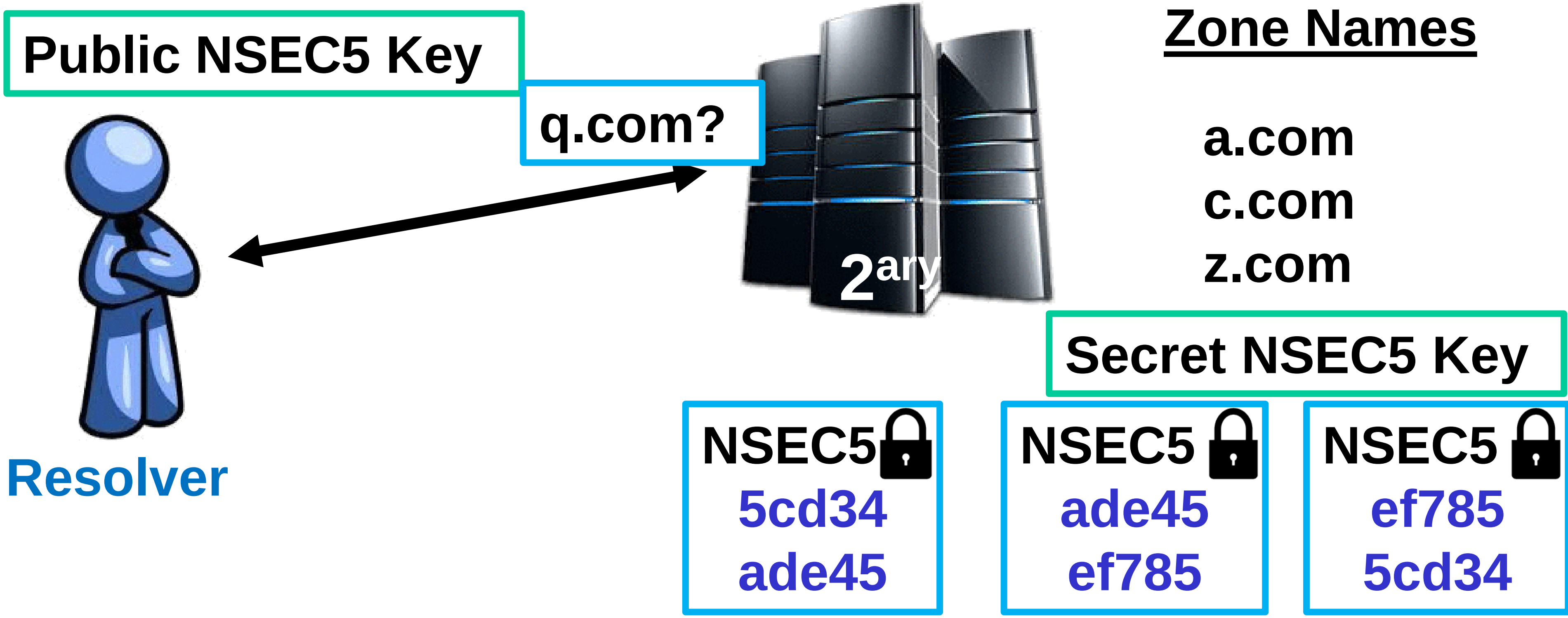
Zone Names

a.com
c.com
z.com

Secret NSEC5 Key

NSEC5 🔒	NSEC5 🔒	NSEC5 🔒
5cd34	ade45	ef785
ade45	ef785	5cd34

NSEC5 in action



Public NSEC5 Key

q.com?

Resolver

2^{ary}

Zone Names

a.com
c.com
z.com

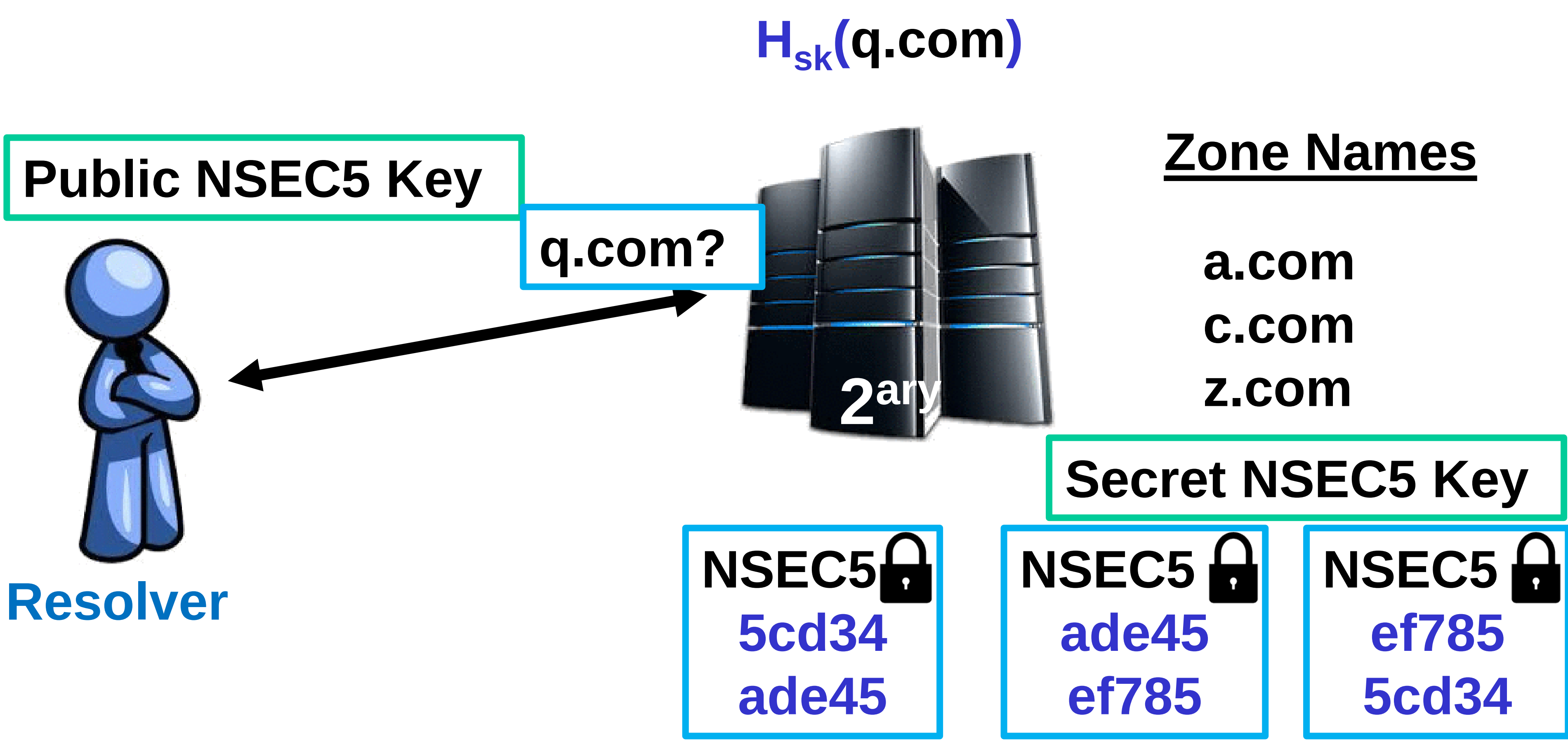
Secret NSEC5 Key

NSEC5
5cd34
ade45

NSEC5
ade45
ef785

NSEC5
ef785
5cd34

NSEC5 in action



H_{sk}(q.com)

Public NSEC5 Key

q.com?

Resolver

Zone Names

a.com
c.com
z.com

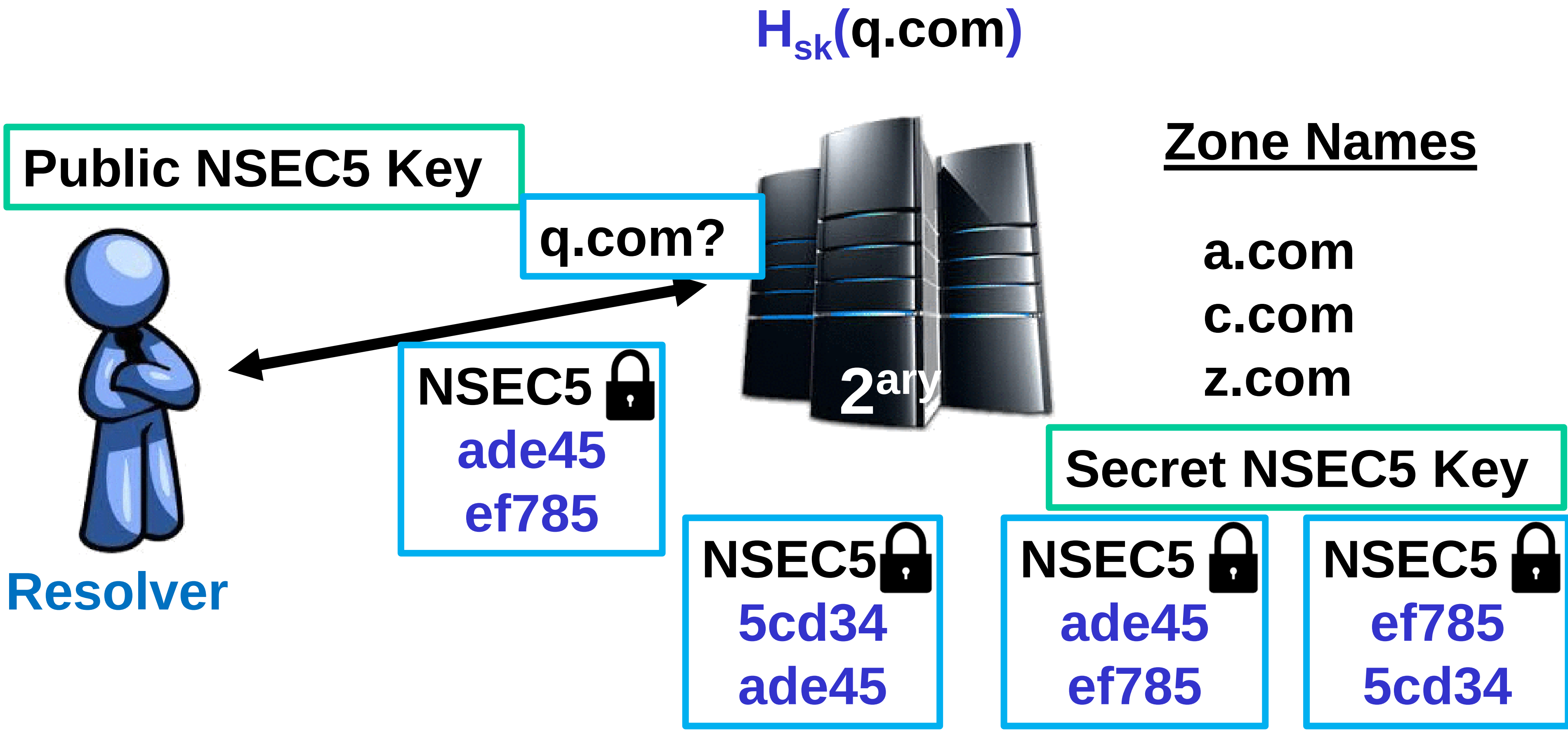
Secret NSEC5 Key

NSEC5 🔒
5cd34
ade45

NSEC5 🔒
ade45
ef785

NSEC5 🔒
ef785
5cd34

NSEC5 in action



H_{sk}(q.com)

Public NSEC5 Key

q.com?

NSEC5
ade45
ef785

Resolver

Zone Names

a.com
c.com
z.com

Secret NSEC5 Key

NSEC5
5cd34
ade45

NSEC5
ade45
ef785

NSEC5
ef785
5cd34

NSEC5 in action

H_{sk}(q.com)

PROOF

Public NSEC5 Key

q.com?

Resolver

NSEC5 🔒
ade45
ef785

Zone Names

a.com
c.com
z.com

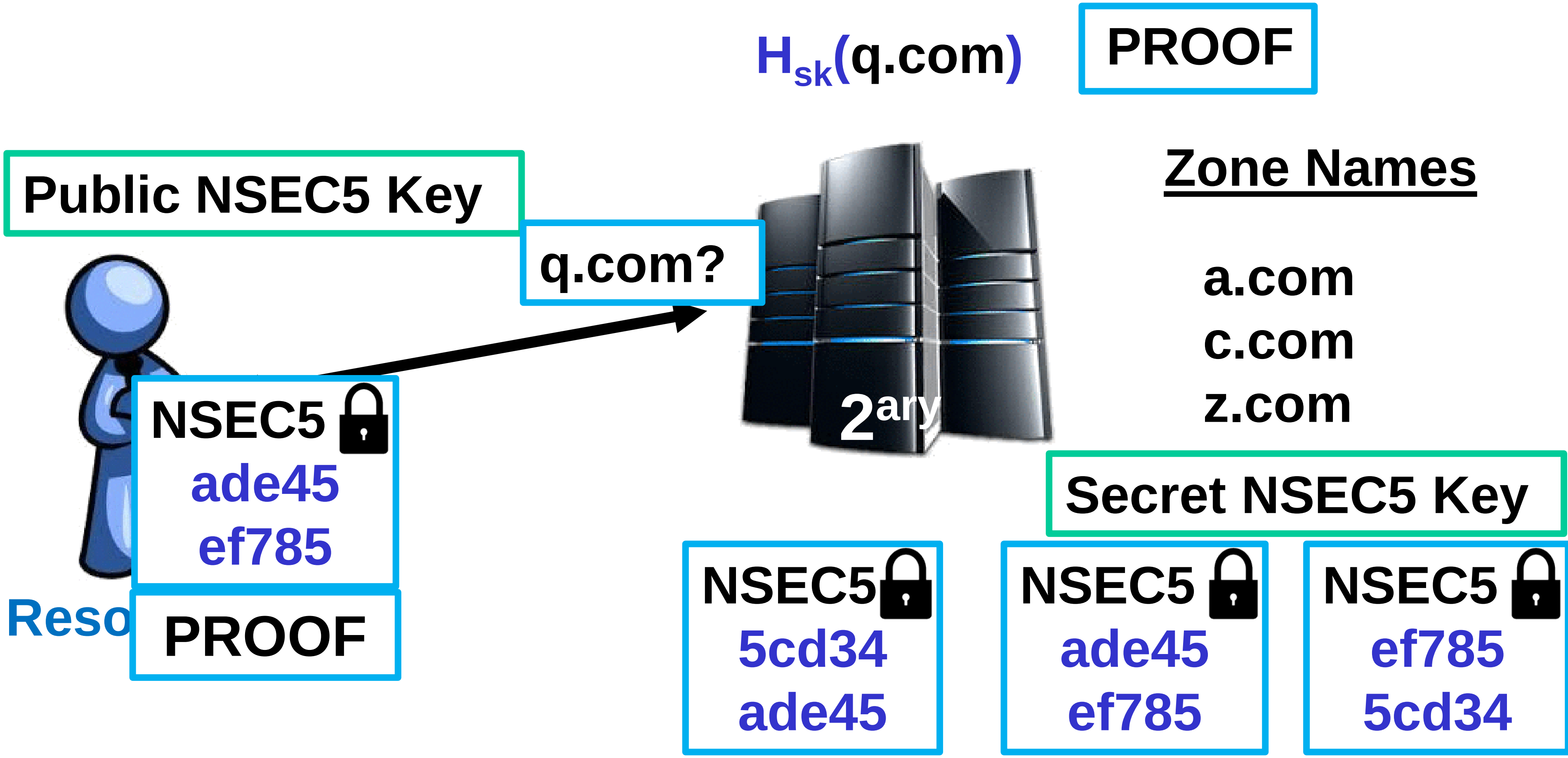
Secret NSEC5 Key

NSEC5 🔒
5cd34
ade45

NSEC5 🔒
ade45
ef785

NSEC5 🔒
ef785
5cd34

NSEC5 in action



H_{sk}(q.com)

PROOF

Zone Names

a.com
c.com
z.com

Public NSEC5 Key

q.com?

2^{ary}

Secret NSEC5 Key

NSEC5 🔒
ade45
ef785

Reso

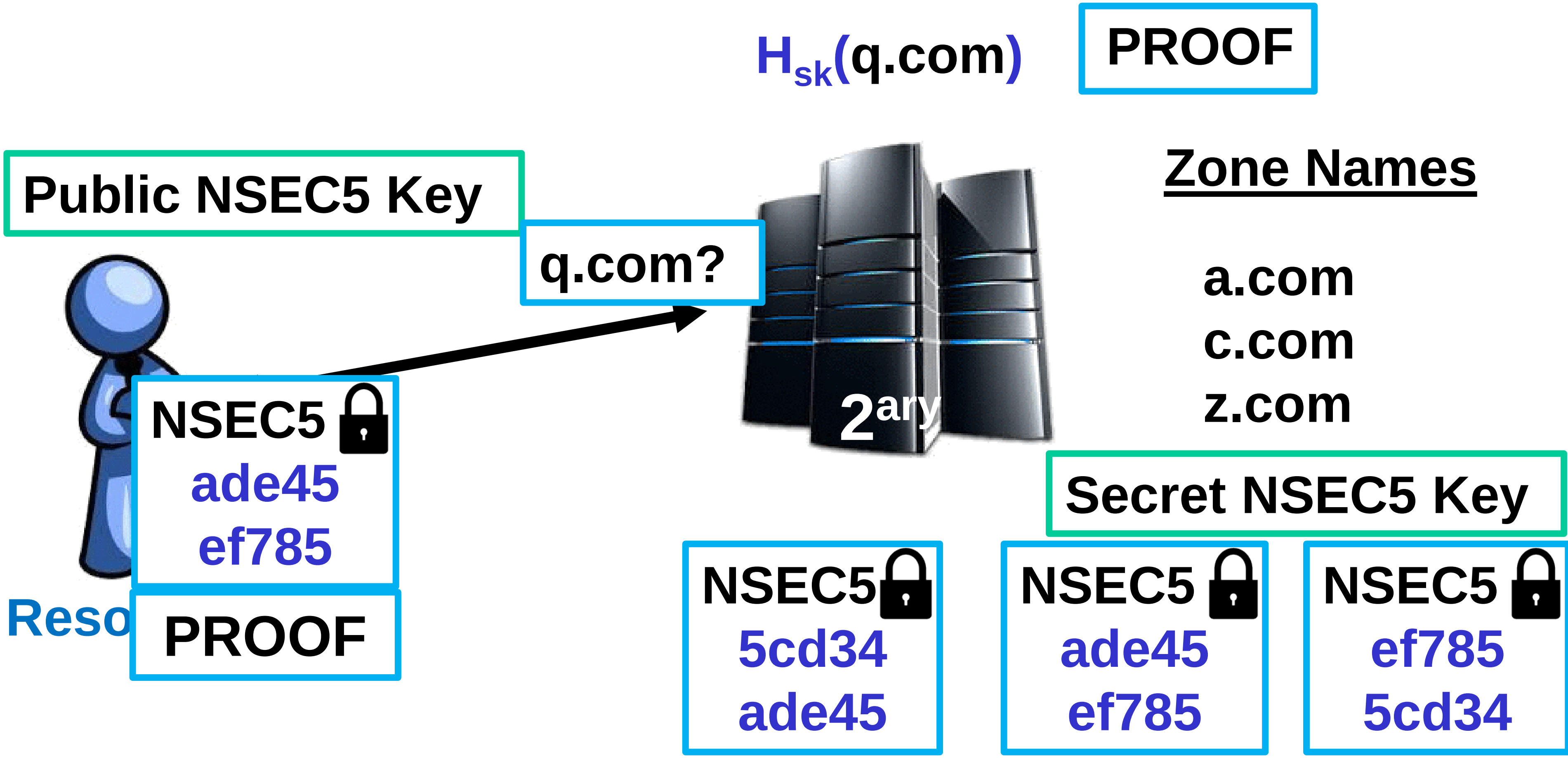
PROOF

NSEC5 🔒
5cd34
ade45

NSEC5 🔒
ade45
ef785

NSEC5 🔒
ef785
5cd34

NSEC5 in action



H_{sk}(q.com)

PROOF

Public NSEC5 Key

q.com?

2ary

Zone Names

a.com
c.com
z.com

Secret NSEC5 Key

NSEC5
ade45
ef785

Reso

PROOF

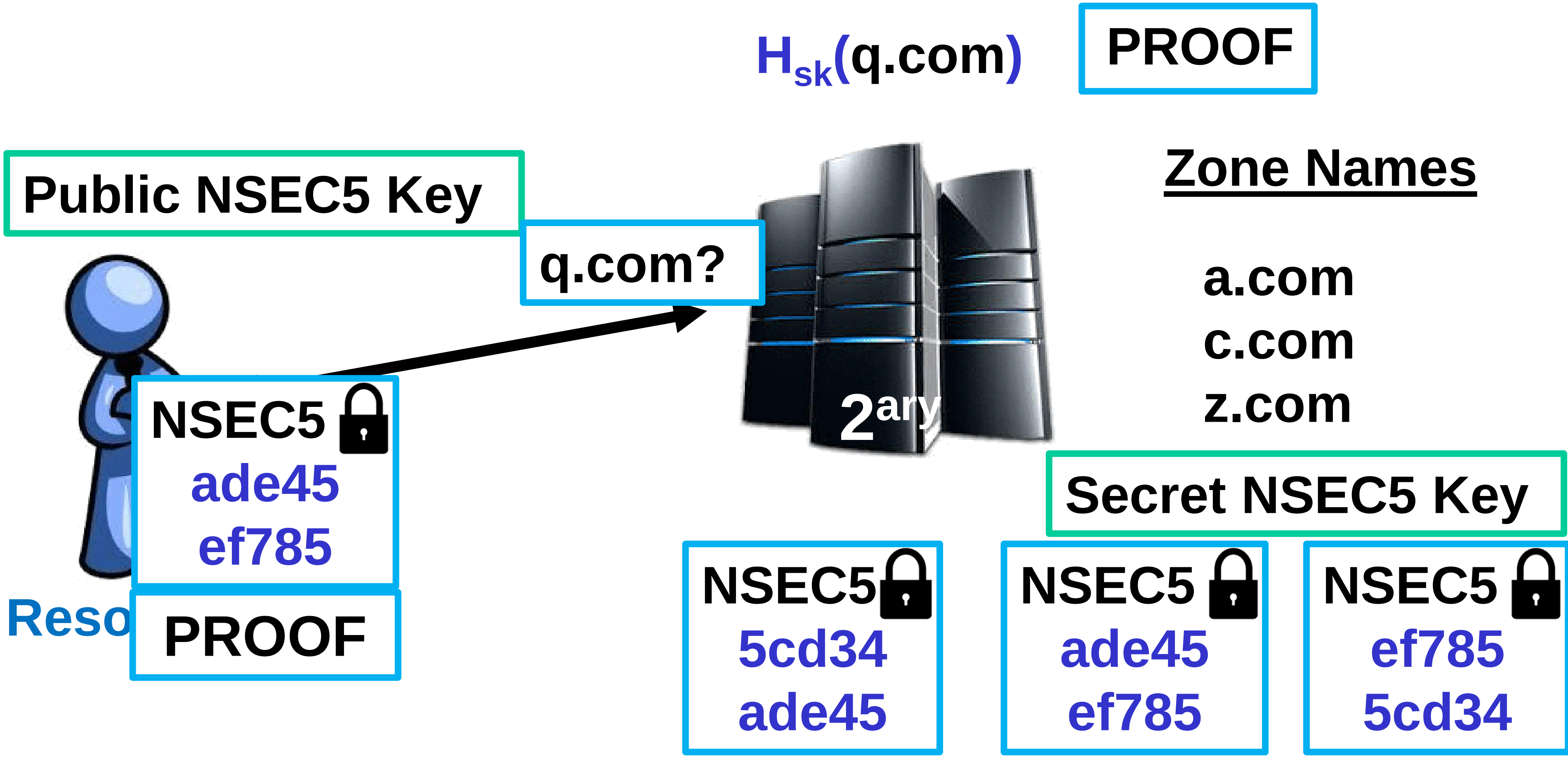
NSEC5
5cd34
ade45

NSEC5
ade45
ef785

NSEC5
ef785
5cd34

1. Verify H_{sk}(q.com) was computed **correctly** using **public NSEC5 key**

NSEC5 in action



H_{sk}(q.com)

PROOF

Public NSEC5 Key

q.com?

Zone Names

a.com
c.com
z.com

NSEC5
ade45
ef785

2^{ary}

Secret NSEC5 Key

Reso

PROOF

NSEC5
5cd34
ade45

NSEC5
ade45
ef785

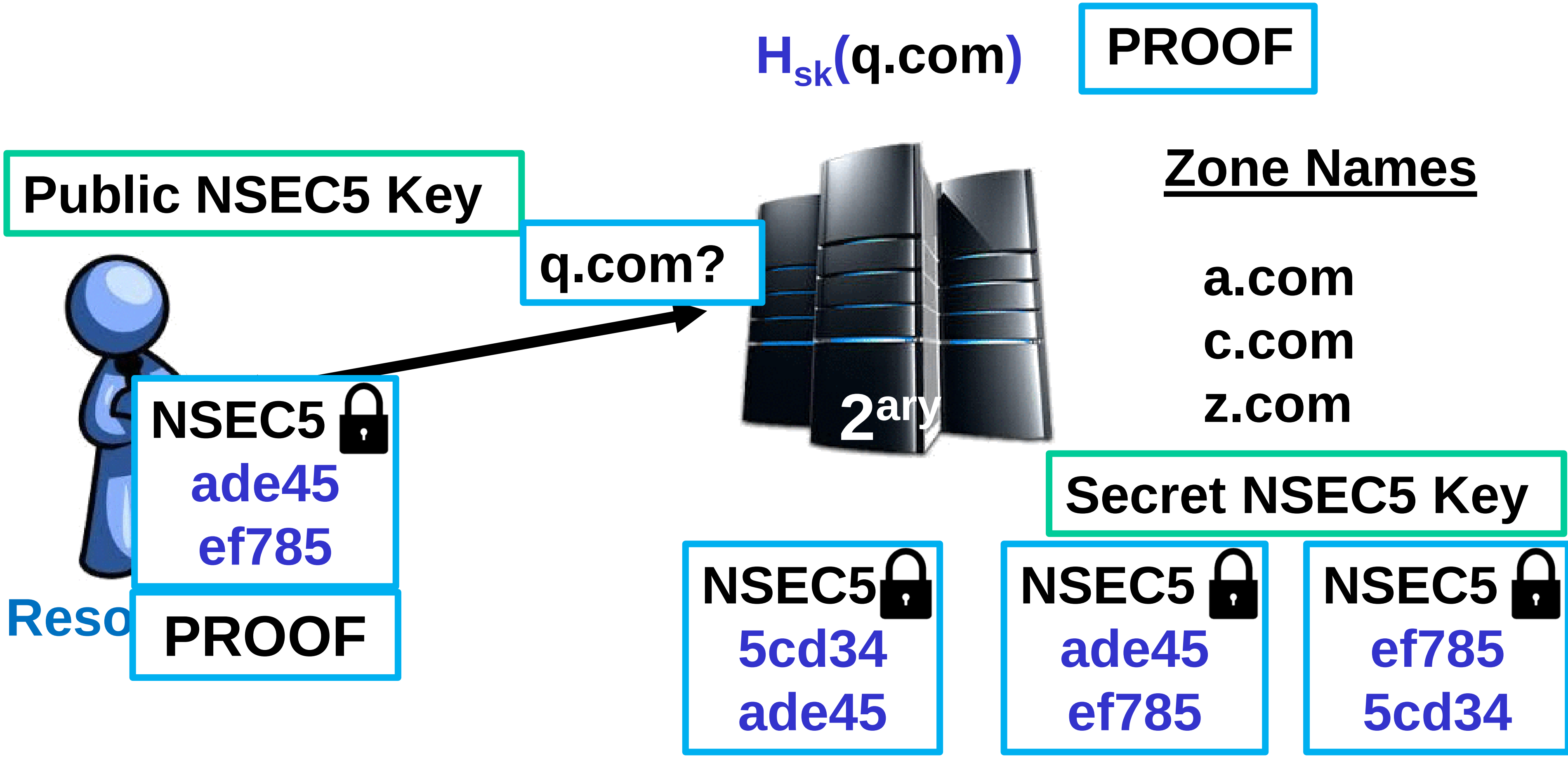
NSEC5
ef785
5cd34

1. **Verify H_{sk}(q.com)** was computed

correctly using **public NSEC5 key**

2. ade45 < H_{sk}(q.com) < ef785

NSEC5 in action



H_{sk}(q.com) PROOF

Public NSEC5 Key

q.com?

NSEC5
ade45
ef785

Reso

PROOF

2^{ary}

Zone Names

a.com
c.com
z.com

Secret NSEC5 Key

NSEC5
5cd34
ade45

NSEC5
ade45
ef785

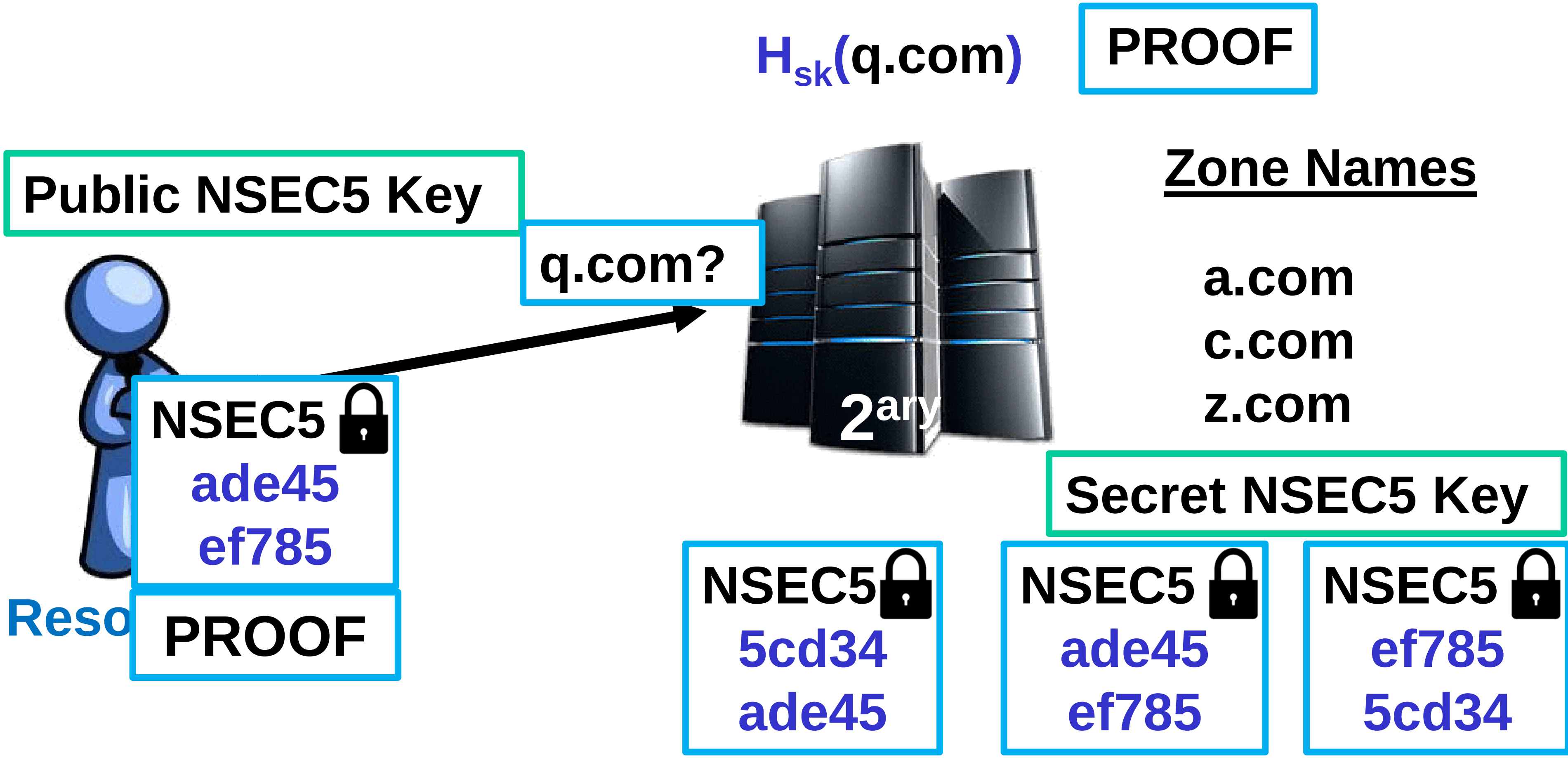
NSEC5
ef785
5cd34

1. **Verify H_{sk}(q.com)** was computed **correctly** using **public NSEC5 key**

2. ade45 < H_{sk}(q.com) < ef785

Integrity?

NSEC5 in action



H_{sk}(q.com)

PROOF

Public NSEC5 Key

q.com?

Zone Names

a.com
c.com
z.com

2ary

NSEC5
ade45
ef785

Reso

PROOF

Secret NSEC5 Key

NSEC5
5cd34
ade45

NSEC5
ade45
ef785

NSEC5
ef785
5cd34

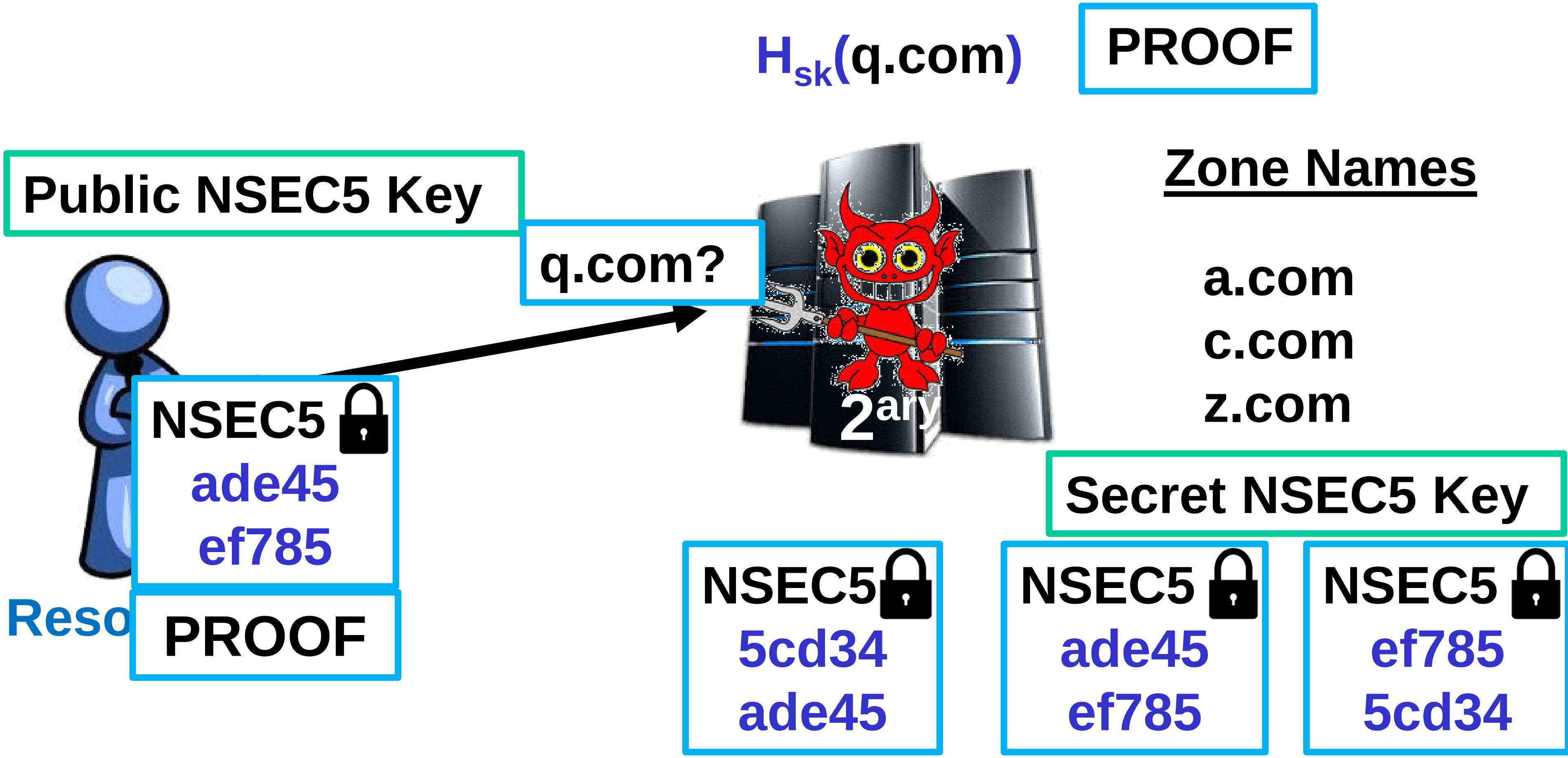
1. **Verify** H_{sk}**(q.com)** was computed **correctly** using **public NSEC5 key**

2. **ade45 <** H_{sk}**(q.com) < ef785**

Integrity?

Privacy?

NSEC5 in action



H_{sk}(q.com) PROOF

Public NSEC5 Key

q.com?

Zone Names

a.com
c.com
z.com

NSEC5
ade45
ef785

Reso

PROOF

2ary

Secret NSEC5 Key

NSEC5
5cd34
ade45

NSEC5
ade45
ef785

NSEC5
ef785
5cd34

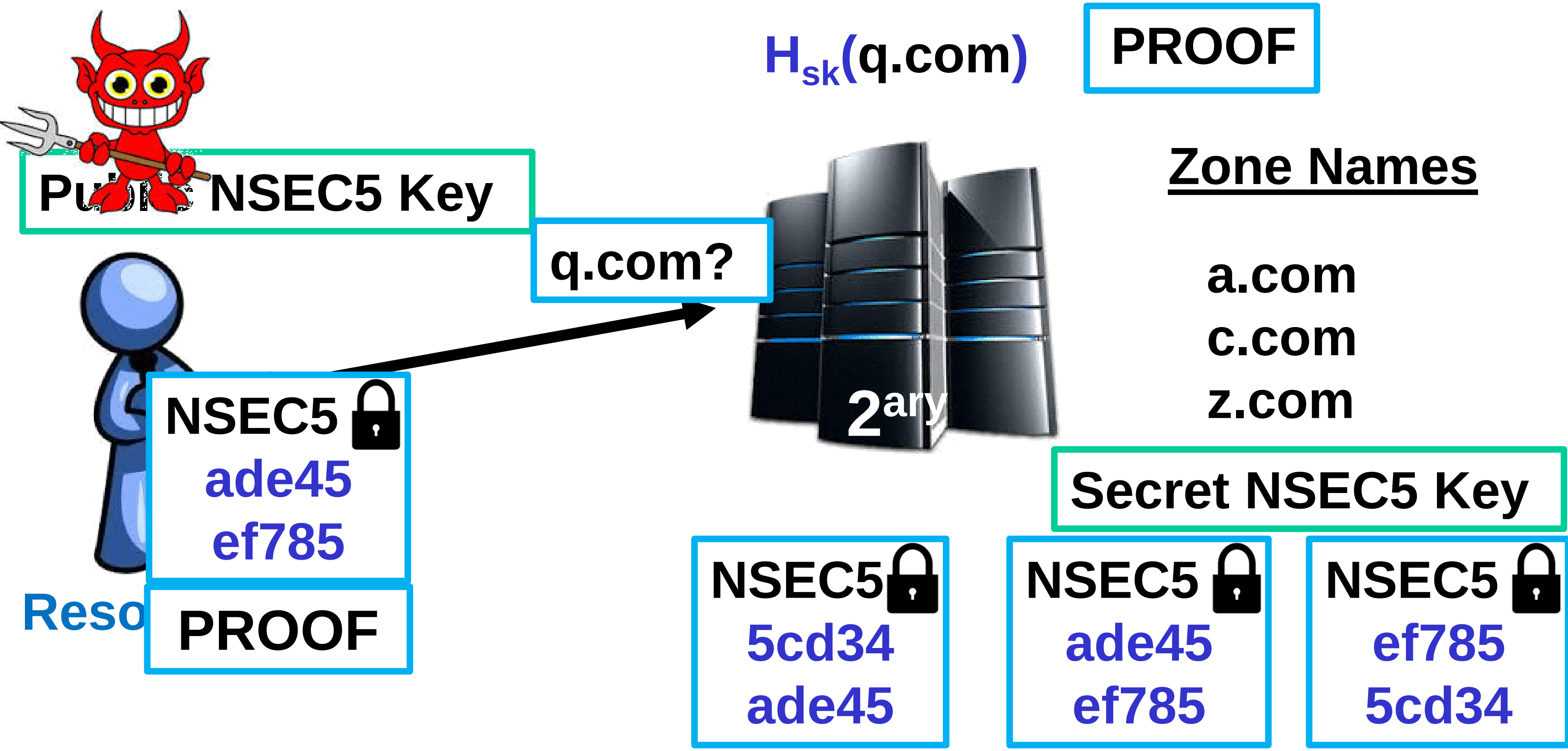
1. **Verify** H_{sk}**(q.com)** was computed **correctly** using **public NSEC5 key**

2. ade45 < H_{sk}(q.com) < ef785

Integrity? Yes!

Privacy?

NSEC5 in action



Public NSEC5 Key

q.com?

NSEC5 🔒
ade45
ef785

Reso

PROOF

H_{sk}(q.com)

PROOF

2ary

Zone Names

a.com
c.com
z.com

Secret NSEC5 Key

NSEC5 🔒
5cd34
ade45

NSEC5 🔒
ade45
ef785

NSEC5 🔒
ef785
5cd34

1. **Verify** H_{sk}**(q.com)** was computed **correctly** using **public NSEC5 key**

2. ade45 < H_{sk}(q.com) < ef785

Integrity? Yes!

Privacy? Yes!

NSEC5 – Implementing the keyed hash function

NSEC5 – Implementing the keyed hash function

NSEC5 -

a.com

NSEC5 – Implementing the keyed hash function

NSEC5 - **h_1(a.com)**

NSEC5 – Implementing the keyed hash function

NSEC5 - $\mathrm{RSA}_{SK}(h_1(\mathrm{a.com}))$

NSEC5 – Implementing the keyed hash function

NSEC5 - $\mathrm{RSA}_{SK}(h_1(\text{a.com}))$

$$\mathrm{RSA}_{SK}(x) = x^d \mod N$$

NSEC5 – Implementing the keyed hash function

NSEC5 - $\mathrm{RSA}_{SK}(h_1(\mathrm{a.com}))$

$$\mathrm{RSA}_{SK}(x) = x^{d} \bmod N$$

NSEC5 – Implementing the keyed hash function

NSEC5 - $h_2(RSA_{SK}(h_1(a.com)))$

$$RSA_{SK}(x) = x^d \bmod N$$

NSEC5 – Implementing the keyed hash function

NSEC5 - $h_2(RSA_{SK}(h_1(a.com)))$

$$RSA_{\boxed{SK}}(x) = x^{\boxed{d}} \bmod \boxed{N}$$

NSEC3 - $h_2(a.com)$ **(SHA256)**

NSEC5 – Implementing the keyed hash function

NSEC5 - $H_{sk}(\text{a.com})=h_2(RSA_{SK}(h_1(\text{a.com})))$

$$RSA_{SK}(x)= x^{d} \bmod N$$

NSEC3 - $h_2(\text{a.com})$ **(SHA256)**

NSEC5 – Implementing the keyed hash function

NSEC5 - $H_{sk}(\text{a.com})=h_2(\underbrace{RSA_{SK}(h_1(\text{a.com}))}_{\text{(“Full Domain Hash” [BR93])}})$

$$RSA_{SK}(x)= x^{d} \bmod N$$

NSEC3 - $h_2(\text{a.com})$ **(SHA256)**

NSEC5 – Implementing the keyed hash function

H_{sk} **is a Verifiable Random Function (VRF) [MRV99]**

$$\textbf{NSEC5 -}\ H_{sk}(a.com)=\overbrace{h_2(\underbrace{RSA_{SK}(h_1(a.com))}_{\text{(“Full Domain Hash” [BR93])}})}^{\textbf{VRF}}$$

$$RSA_{SK}(x)= x^{d} \bmod N$$

$$\textbf{NSEC3 -}\ h_2(a.com) \qquad \textbf{(SHA256)}$$

NSEC5 – Implementing the keyed hash function

H_{sk} is a Verifiable Random Function (VRF) [MRV99]

$$\text{NSEC5 - } H_{sk}(a.com)=\overbrace{h_2(\underbrace{RSA_{SK}(h_1(a.com))}_{\text{PROOF } \pi})}^{\text{VRF}}$$

$$RSA_{SK}(x)= x^{d} \bmod N$$

$$\text{NSEC3 - } h_2(a.com) \qquad \text{(SHA256)}$$

NSEC5 – Implementing the keyed hash function

H_{sk} **is a Verifiable Random Function (VRF) [MRV99]**

$$\textbf{NSEC5 - } H_{sk}(a.com)=\overbrace{h_2(\underbrace{RSA_{SK}(h_1(a.com))}_{\textbf{PROOF } \pi})}^{\textbf{VRF}}$$

$$RSA_{SK}(x)= x^d \bmod N$$

$$RSA_{PK}(\pi)= \pi^e \bmod N \equiv x$$

$$\textbf{NSEC3 - } h_2(a.com) \qquad \textbf{(SHA256)}$$

NSEC5 – Implementing the keyed hash function

H_{sk} is a Verifiable Random Function (VRF) [MRV99]

$$\textbf{NSEC5 - } H_{sk}(\text{a.com}) = \overbrace{h_2(\underbrace{\text{RSA}_{SK}(h_1(\text{a.com}))}_{\text{PROOF } \pi})}^{\text{VRF}}$$

$$\text{RSA}_{SK}(x) = x^{d} \bmod N$$

$$\text{RSA}_{PK}(\pi) = \pi^{e} \bmod N \equiv x$$

NSEC3 - h_2(a.com) **(SHA256)**

Summary

	Integrity against outsiders	Integrity against compromised 2^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

Summary

	Integrity against outsiders	Integrity against compromised 2dry nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗
NSEC5	✓	✓	✓

Summary

	Integrity against outsiders	Integrity against compromised 2^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗
NSEC5	✓	✓	✓
NSEC5; lost secret N5K	✓	✓	✗

Summary

	Integrity against outsiders	Integrity against compromised 2dry nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗
NSEC5	✓	✓	✓
NSEC5; lost secret N5K	✓	✓	✗

Just like NSEC3!

Lower bound

NSEC5 uses RSA computations online!

Lower bound

NSEC5 uses RSA computations online!

- Is this really necessary?

Lower bound

NSEC5 uses RSA computations online!

- Is this really necessary?

- Unfortunately yes! ☹

Lower bound

NSEC5 uses RSA computations online!

- Is this really necessary?

- Unfortunately yes! ☹

Theorem [Informal]: ANY denial of existence scheme that

1. prevents **zone enumeration**, and
2. provides **integrity** against network attackers

requires nameservers to perform **public-key operations** for every negative response.

Lower bound

NSEC5 uses RSA computations online!

- Is this really necessary?

- Unfortunately yes! ☹

Theorem [Informal]: ANY denial of existence scheme that

1. prevents **zone enumeration**, and
2. provides **integrity** against network attackers

requires nameservers to perform **public-key operations** for every negative response.

→Explains why NSEC3 is still vulnerable to zone enumeration.

Lower bound

NSEC5 uses RSA computations online!

- Is this really necessary?

- Unfortunately yes! ☹

Theorem [Informal]: ANY denial of existence scheme that

1. prevents **zone enumeration**, and
2. provides **integrity** against network attackers

requires nameservers to perform **public-key operations** for every negative response.

→Explains why NSEC3 is still vulnerable to zone enumeration.

(NSEC5 is **optimal -** requires only **one** RSA computation)

Conclusion

This work

- proposes NSEC5

  first DNSSEC scheme that prevents zone enumeration
  while maintaining integrity for a compromised nameserver

- proves that zone-enumeration

  cannot be avoided without online public-key operations

- we would like to implement NSEC5

  we are writing an Internet draft
  give us your feedback and suggestions!

Project webpage:
http://www.cs.bu.edu/~goldbe/papers/nsec5.html

Conclusion

This work

- proposes NSEC5

  first DNSSEC scheme that prevents zone enumeration
  while maintaining integrity for a compromised nameserver

- proves that zone-enumeration

  cannot be avoided without online public-key operations

- we would like to implement NSEC5

  we are writing an Internet draft
  give us your feedback and suggestions!

Project webpage:
http://www.cs.bu.edu/~goldbe/papers/nsec5.html

THANK YOU!