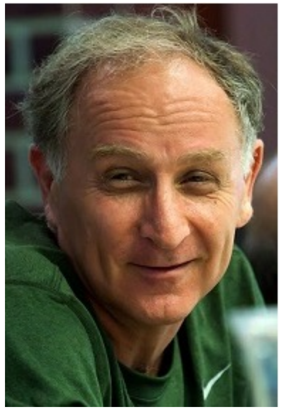
AdaDoQ: Adaptive DNSSEC



Yehuda Afek
Tel-Aviv University

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Anat Bremler-Barr
Reichman University

IDC HERZLIYA

Daniel Dubnikov
Tel-Aviv University

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Supported By:

ICRC Blavatnik Interdisciplinary Cyber Research Center

GÉANT

Motivation

- DNSSEC is important
- DNS with DNSSEC does not scale, specifically,

  ➔Vulnerable to NXDomain flood attacks

Goal

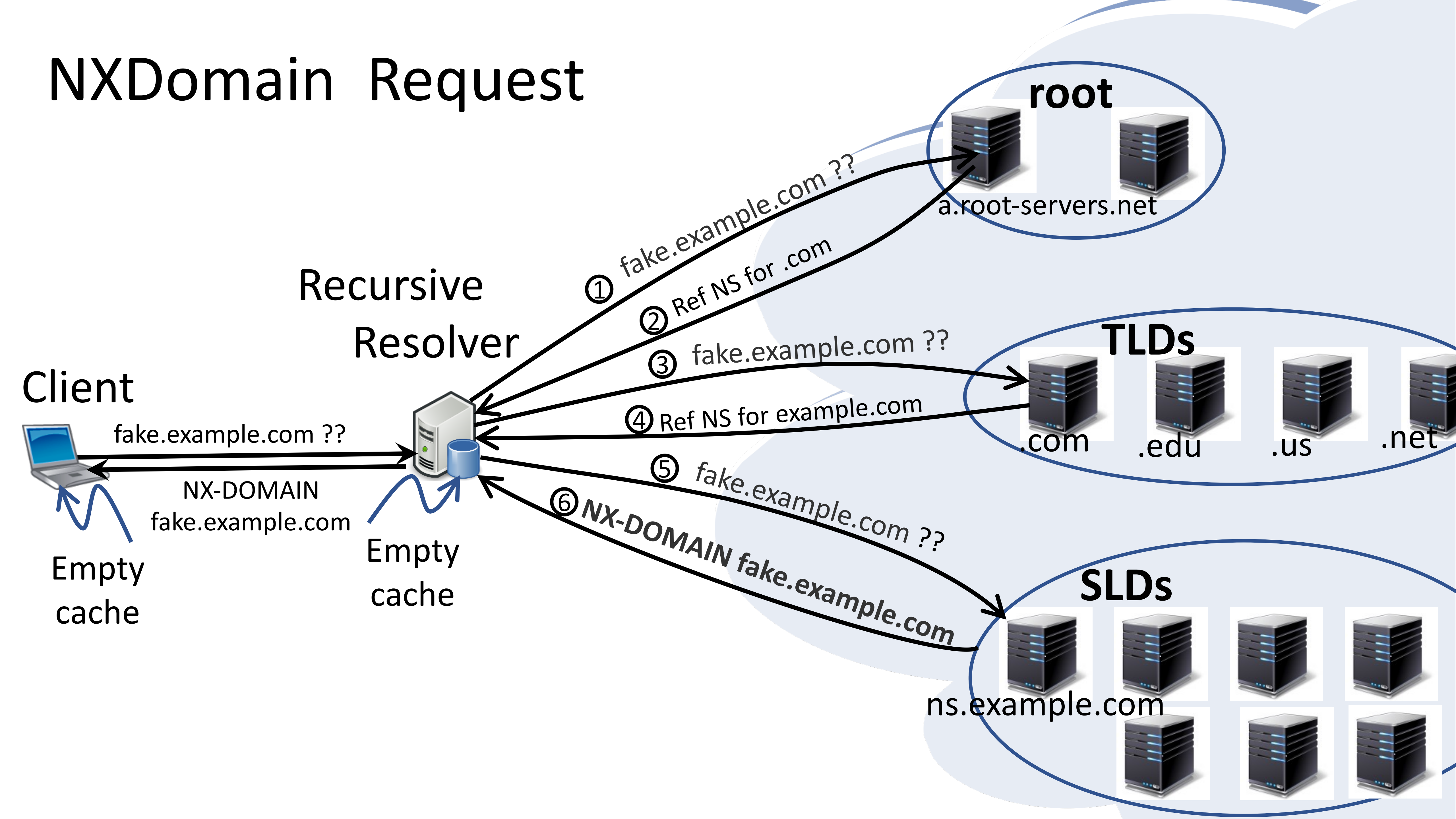
1. To measure DNSSEC scalability relative to Plain DNS
2. Develop a method for <resolver ←→ authoritative> collaboration that is (a) Scalable, (b) as secure as DNSSEC, and (c) introduces no new vulnerabilities.

   a. Provides the same security level as DNSSEC, and
   b. Provides performances close to that of Plain-DNS, and
   c. Does not enable new vulnerabilities.

Outline

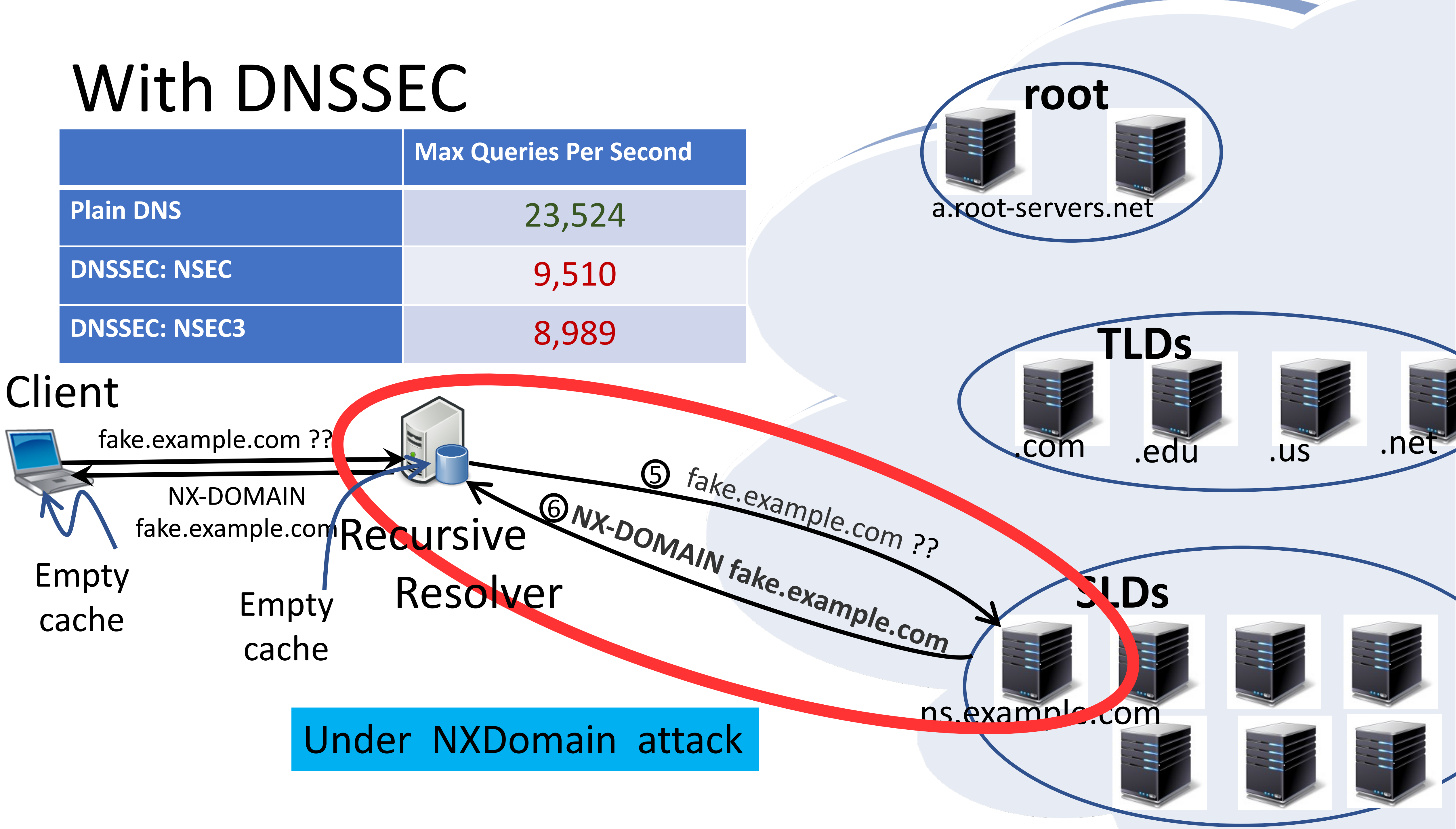
- Motivation: DNSSEC under NXDomain flood attack
  - Either slow or Zone walking vulnerability
- AdaDoQ: solution:
  - TCP/TLS
  - DNSSEC PKI hierarchy of trust
  - QUIC
- AdaDoQ performances
- Conclusions

NXDomain Request



With DNSSEC

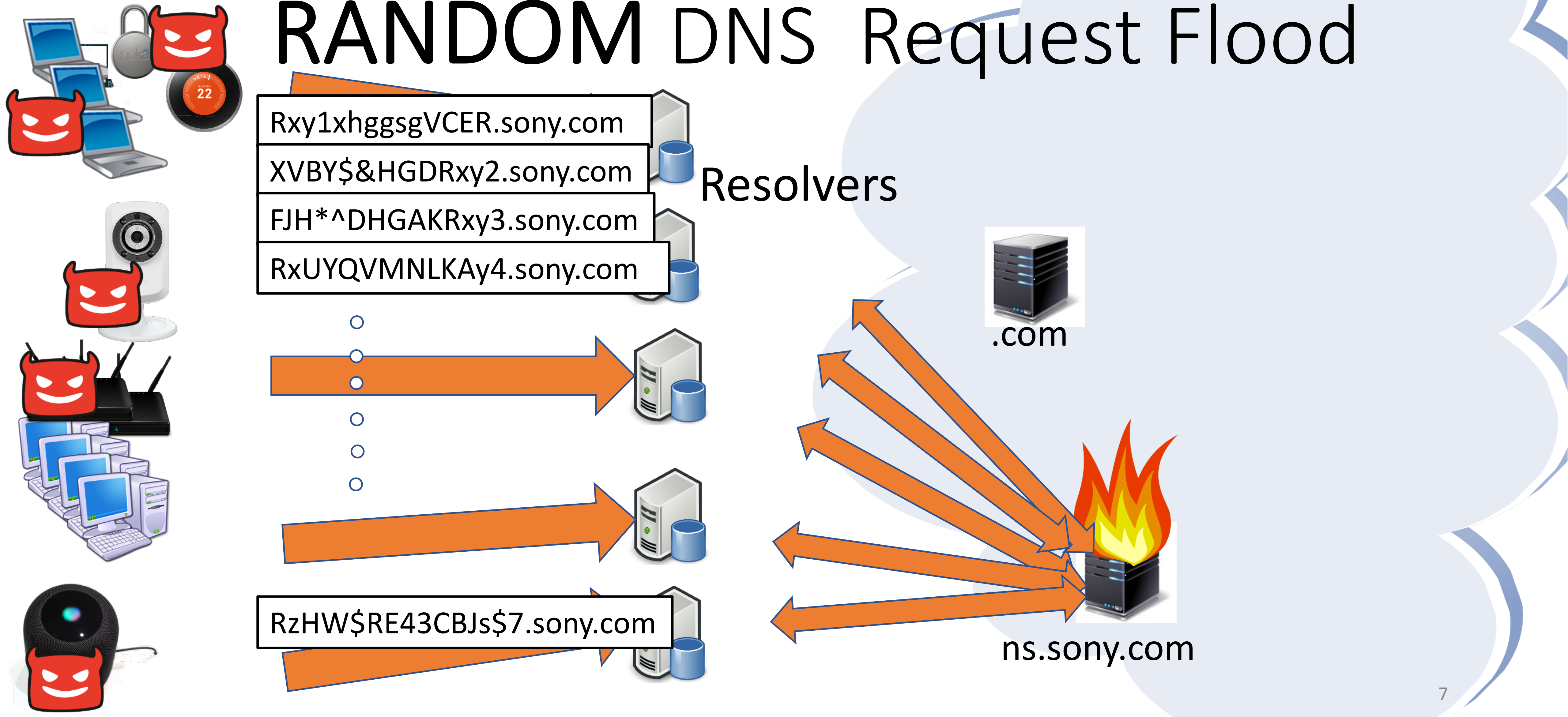
	Max Queries Per Second
Plain DNS	23,524
DNSSEC: NSEC	9,510
DNSSEC: NSEC3	8,989



Under NXDomain attack

NXDomain Attack

RANDOM DNS Request Flood



Motivation (1) NSEC aggressive caching

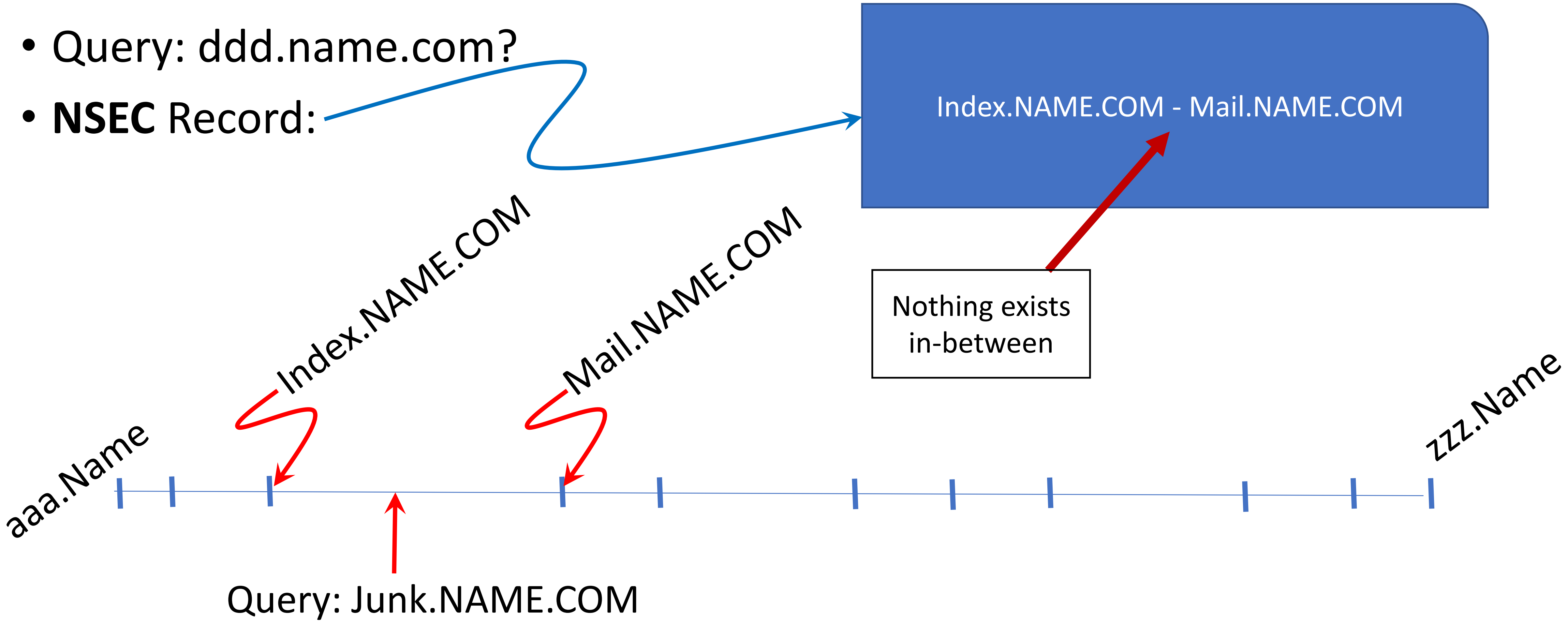
- Non Existent query in DNSSEC?

Motivation (2)

- Non Existent query in DNSSEC?
- Query: ddd.name.com?

Motivation (2) - **NSEC** record

- Non Existent in DNSSEC?
- Query: ddd.name.com?
- **NSEC** Record:



Motivation (2) NSEC aggressive caching

- Aggressive Caching (RFC 8198) – stops NX Attack

	Max Queries Per Second
Plain DNS	23,524
DNSSEC: NSEC	9,510
DNSSEC: NSEC3	8,989
Aggressive Caching	**Max Queries Per Second**
DNSSEC: NSEC	96,226
DNSSEC: NSEC3	93,756

With Knot

Motivation (2) NSEC aggressive caching

- Aggressive Caching (RFC 8198) – stops NX Attack

	Max Queries Per Second
Plain DNS	23,524
DNSSEC: NSEC	9,510
DNSSEC: NSEC3	8,989
Aggressive Caching	**Max Queries Per Second**
DNSSEC: NSEC	96,226
DNSSEC: NSEC3	93,756

With Knot

Motivation (3) Zone walking

- Aggressive Caching (RFC 8198) – stops NX Attack
- BUT: **Enables Zone Walking**

Index.NAME.COM - Mail.NAME.COM

	Max Queries Per Second
Plain DNS	23,524
DNSSEC: NSEC	9,510
DNSSEC: NSEC3	8,989
Aggressive Caching	**Max Queries Per Second**
DNSSEC: NSEC	96,226
DNSSEC: NSEC3	93,756

With Knot

Motivation (3) Zone walking

- Aggressive Caching (RFC 8198) – stops NX Attack
- BUT: **Enables Zone Walking**

  Scalability Issues: Need to quickly find NSEC record

	Max Queries Per Second
Plain DNS	23,524
DNSSEC: NSEC	9,510
DNSSEC: NSEC3	8,989
Aggressive Caching	**Max Queries Per Second**
DNSSEC: NSEC	96,226
DNSSEC: NSEC3	93,756

With Knot

Motivation (3) Zone walking

- How to stop Zone Walking?

Motivation (3) NSEC3 and Zone walking

- How to stop Zone Walking?

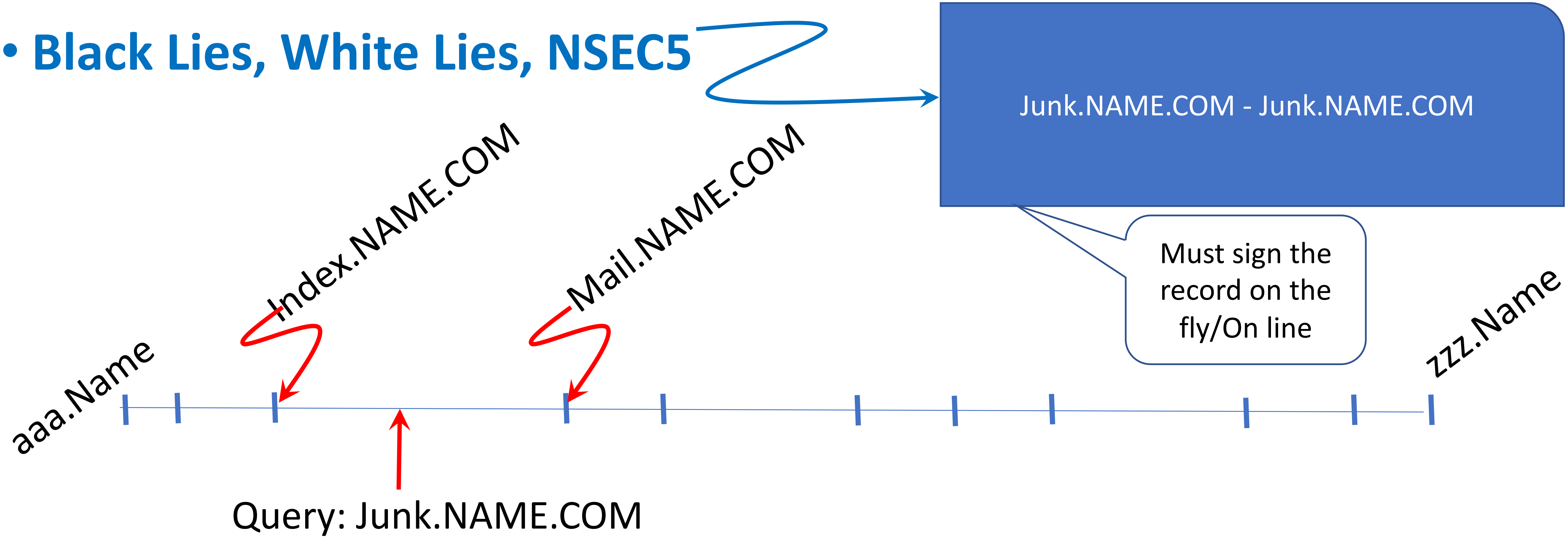
- NSEC3 hash of the interval (the domain names)
  - Keep the hash function on both sides.
  - ➔ Aggressive caching still works. Zone walking is harder, But
  - Still can do Zone Walking with dictionary attack:
    An attacker collects all the NSEC3 records, and uses dictionary attack to reveal the true domain-names

Motivation (3) stop Zone walking by **Black/White lies**

- You can't (without online signing*, Goldberg et al.)

  Nsec5: Provably preventing dnssec zone enumeration

- **Black Lies, White Lies, NSEC5**



Motivation (4)

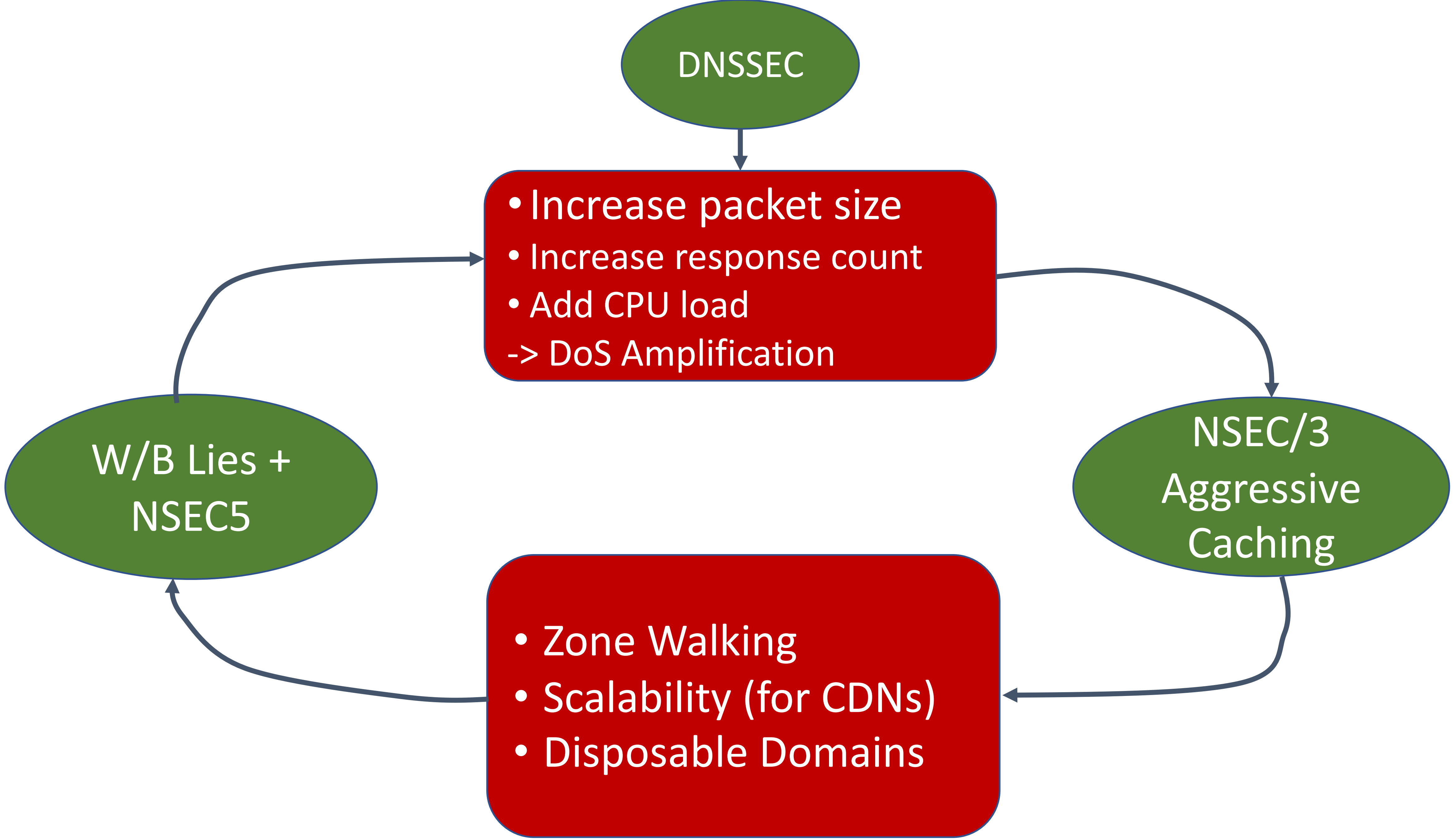
- Online Signing Algorithms – NX Attacks Amplified

	Max Queries Per Second	% of Plain DNS
Plain DNS	23,524	100%
DNSSEC: NSEC	9,510	40%
DNSSEC: NSEC3	8,989	38%
DNSSEC: White Lies	5,863	25%
DNSSEC: Black Lies	7,206	30%
DNSSEC: NSEC5	6,324	27%

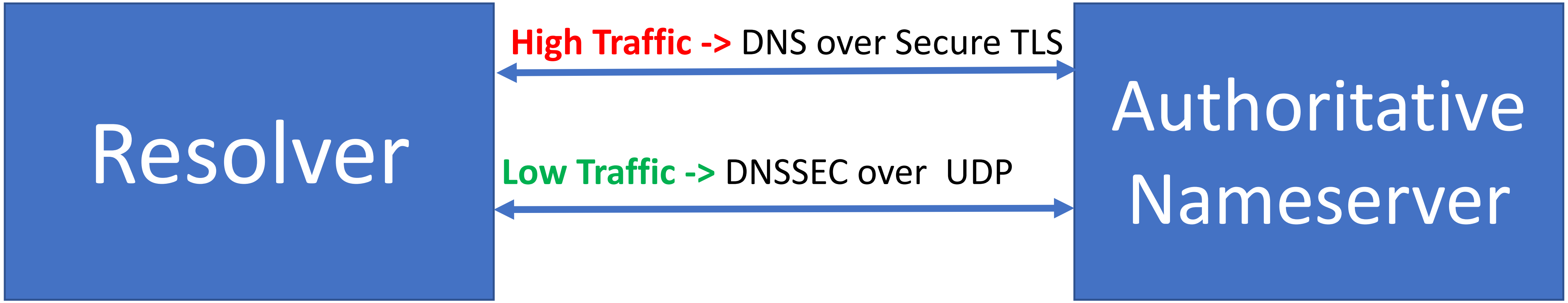
Motivation (4)

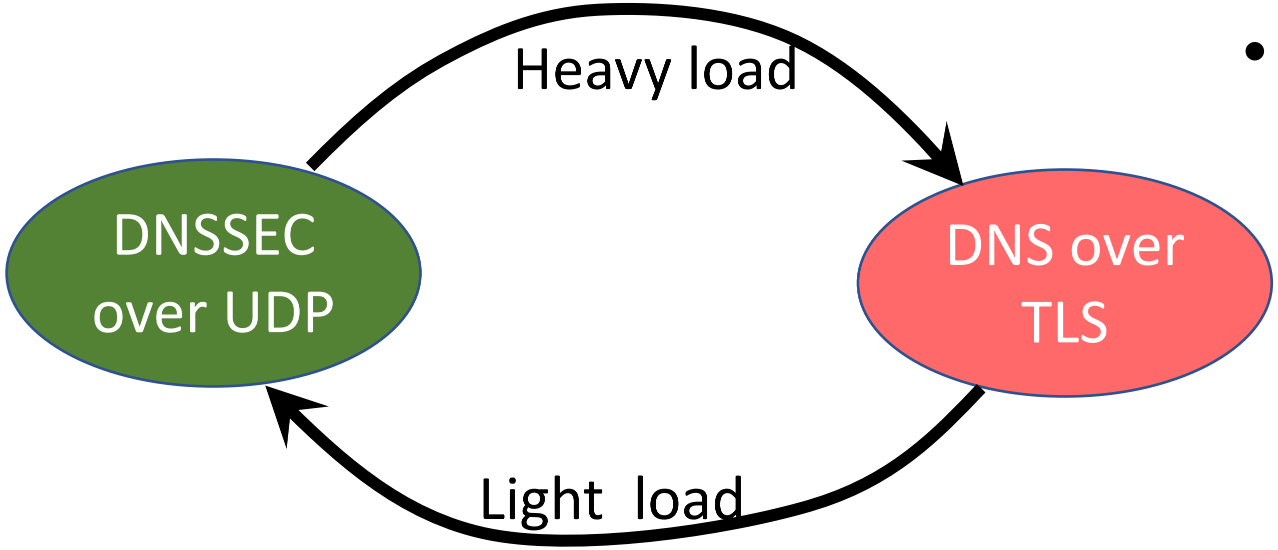
- Online Signing Algorithms – NX Attacks Amplified
- **For security and scalability reasons online signing might be the only option**

	Max Queries Per Second	% of Plain DNS
Plain DNS	23,524	100%
DNSSEC: NSEC	9,510	40%
DNSSEC: NSEC3	8,989	38%
DNSSEC: White Lies	5,863	25%
DNSSEC: Black Lies	7,206	30%
DNSSEC: NSEC5	6,324	27%


DNSSEC
• Increase packet size
• Increase response count
• Add CPU load
-> DoS Amplification
NSEC/3
Aggressive
Caching
• Zone Walking
• Scalability (for CDNs)
• Disposable Domains
W/B Lies +
NSEC5

Proposed Solution - Hybrid





- Authoritative authenticates the resolver once
  - Following traffic is sent without DNSSEC signatures and is considered validated

Proposed Solution (1)

- Remove all DNSSEC overheads
  - Packet Size + extra packet (NSEC record)
  - CPU Load

Proposed Solution (1) TLS

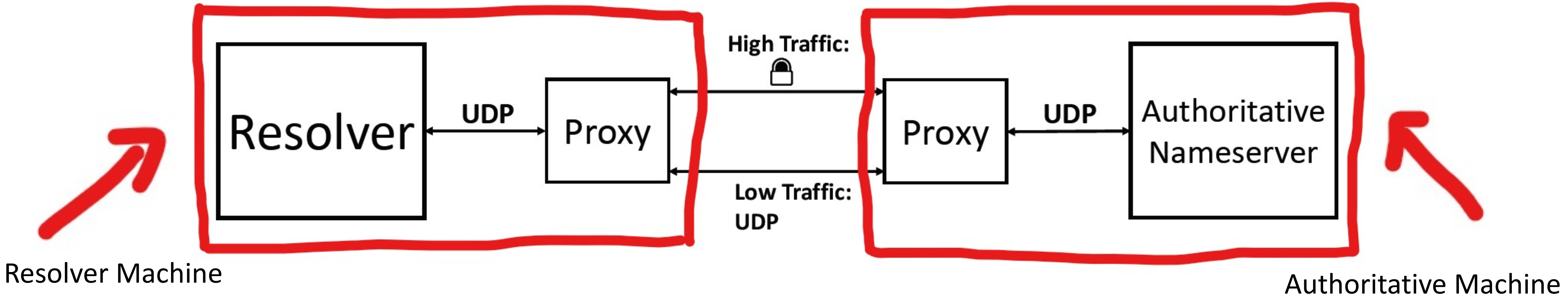
- Remove all DNSSEC overheads
  - Packet Size + Count
  - CPU Load

- Use TLS
  - Resolver initiates
  - Authoritative identifies itself once,
  - Traffic sent with Plain DNS over TLS.
  - **Using **DNSSEC hierarchical chain of trust ** instead of TLS certificates**.
  - **TLS == DNSSEC**: Only owner of DNSSEC key can authenticate information

Proposed Solution – PoC (1) Proxy

- **Problem1:** Can’t easily integrate with known resolver/auth implementations (Bind, Unbound, Knot, etc.)

- **Solution: proxy** interface resolver - authoritative servers



Proposed Solution – PoC (2) **QUIC**

- **Problem2**:
  - TLS overhead is high
  - TLS suffers from Head-of-Line blocking

Proposed Solution – PoC (2) **QUIC**

- **Problem2**:
  - TLS overhead is high
  - TLS suffers from Head-of-Line blocking
- **Solution:** Use **QUIC** (similar to HTTP3)
  - Over UDP
  - UDP Multiplexing (virtual connections) ➔No head of the Line Blocking
  - Connection kept open: resume connection with 0 round trip time
  - No need for TCP integration (firewalls/IPS)
  - At most one QUIC connection for each Resolver-Authoritative pair.

    QUIC anti-spoofing protection

Proposed Solution – PoC (3)

- **Problem3**: Teardown and restart QUIC connections

Proposed Solution – PoC (3) Long lived

- **Problem3**: Teardown and restart QUIC connections
- **Solution:** Keep connections alive
  - QUIC has low overhead – long lived connections
  - QUIC can resume quickly

Proposed Solution – PoC (4)

- **Problem4:** Resource limit

Proposed Solution – PoC (4) Limit # QUIC Connections

- **Problem4:** Resource limit

- **Solution:** Score connection throughput with

$$F_i = \alpha \cdot F_{i-1} + (1 - \alpha) \cdot f_i$$

Exponential Moving Average

➔Resolver terminates lowest scored connection (LRU)

➔Close connection when F_i is below a lower threshold

Proposed Solution – PoC (5) Attack Tolerance

- **Problem5:** Estimate impact of resource exhaustive attacks
- Still need to preform measurement. However:

➔Over UDP instead of TCP

➔Resolver terminates lowest scored connection (LRU).

➔Threshold for closing connection lower than opening threshold

Proposed Solution – PoC (6) No DNSSEC validation

- **Problem6:** Clients cannot validate DNSSEC signatures.

➔Trust the resolver.

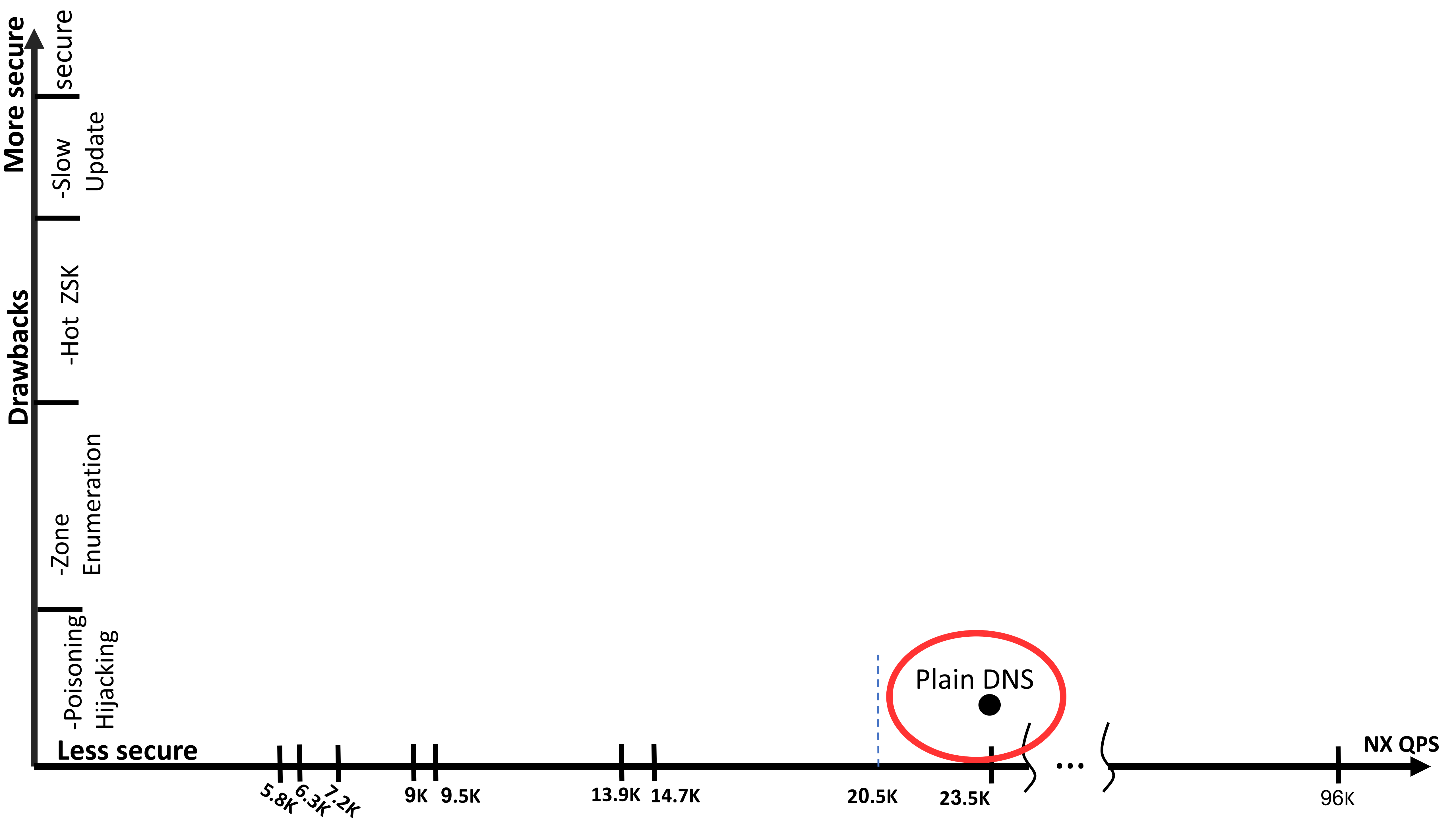
Measurements

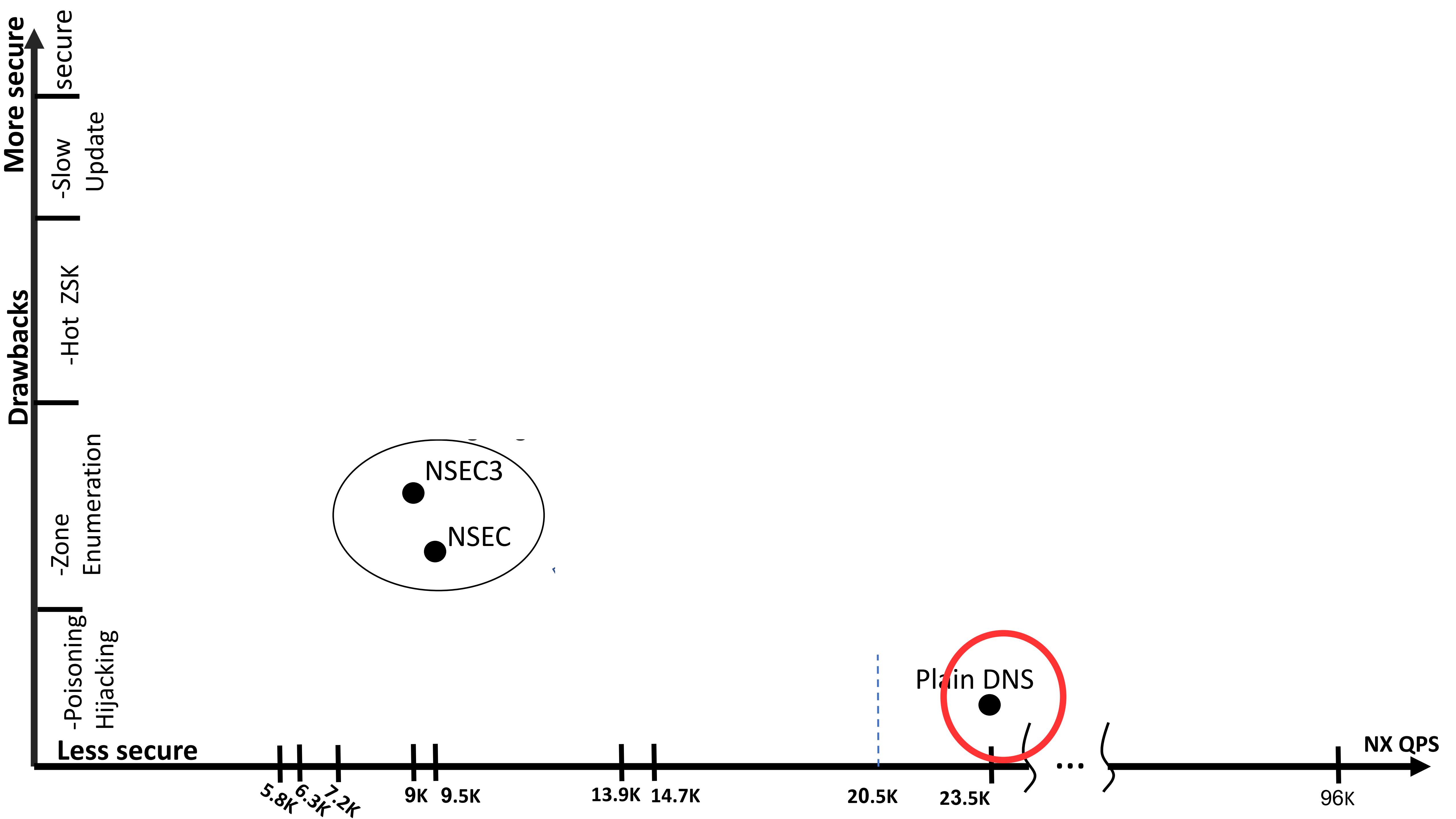
Knot	Max Queries Per Second	% of Plain DNS	ECDSA P-256
Plain DNS	23,524	100%	
DNSSEC: NSEC	9,510	40%	4,213
DNSSEC: NSEC3	8,989	38%	4,015
DNSSEC: White Lies	5,863	25%	2,070
DNSSEC: Black Lies	7,206	30%	3,338
DNSSEC: NSEC5	6,324	27%	2,171

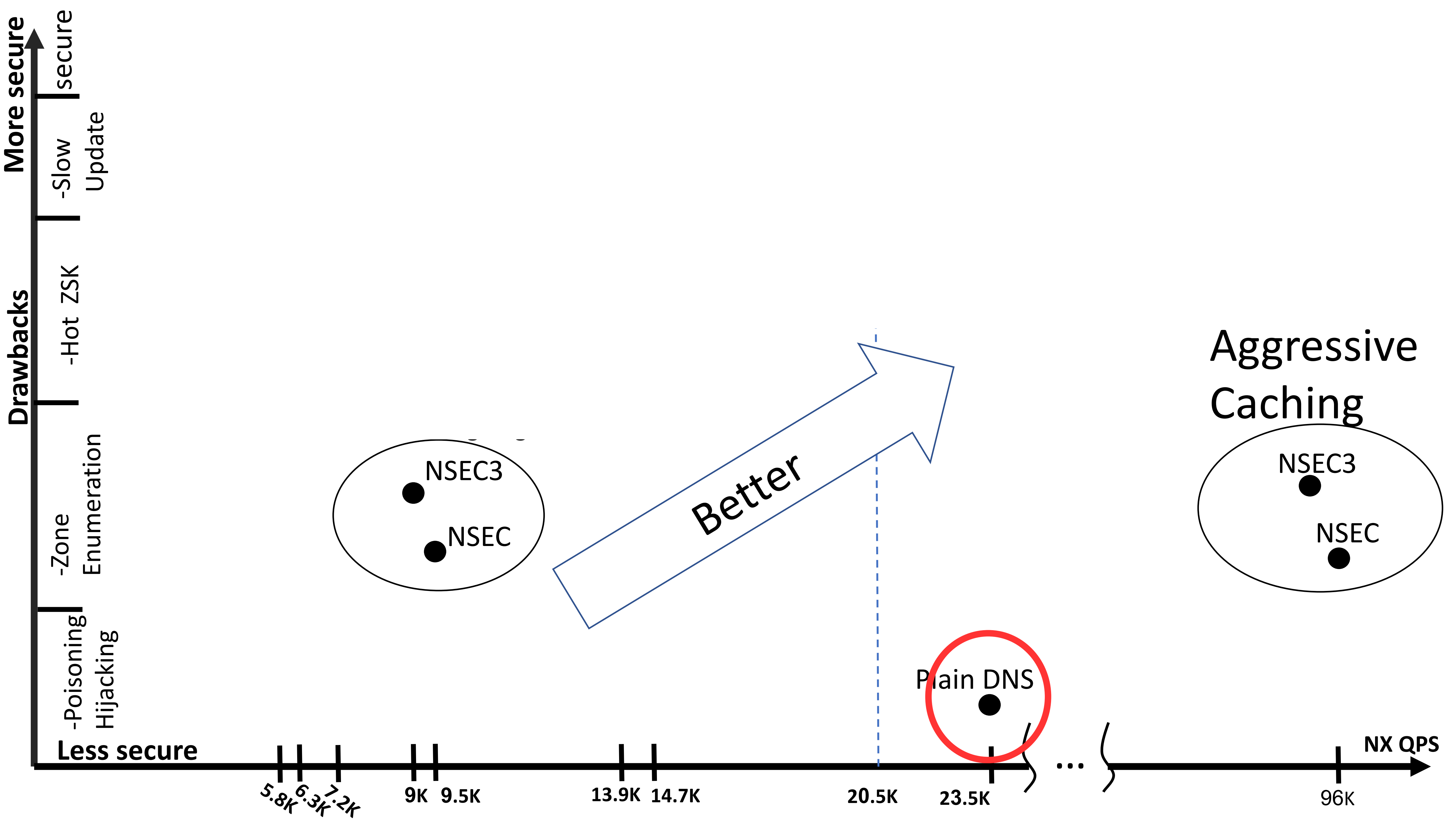
Measurements

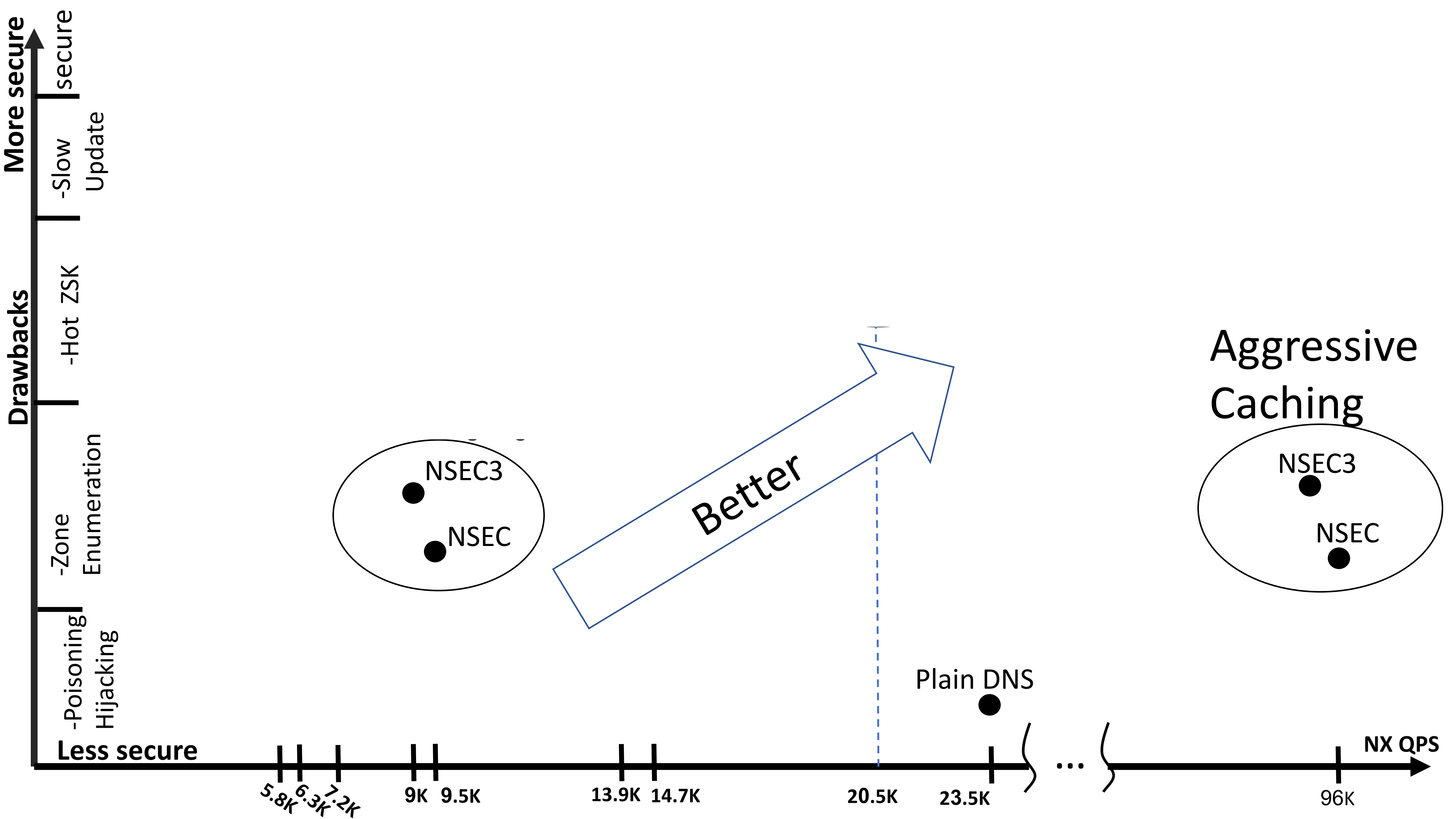
With QUIC, using the same experiment (NX flood), throughput is **87%** of the plain DNS

Knot	Max Queries Per Second	% of Plain DNS	ECDSA P-256
Plain DNS	23,524	100%	
DNSSEC: NSEC	9,510	40%	4,213
DNSSEC: NSEC3	8,989	38%	4,015
DNSSEC: White Lies	5,863	25%	2,070
DNSSEC: Black Lies	7,206	30%	3,338
DNSSEC: NSEC5	6,324	27%	2,171
AdaDoQ (Our Solution)	**20,558**	**87%**	

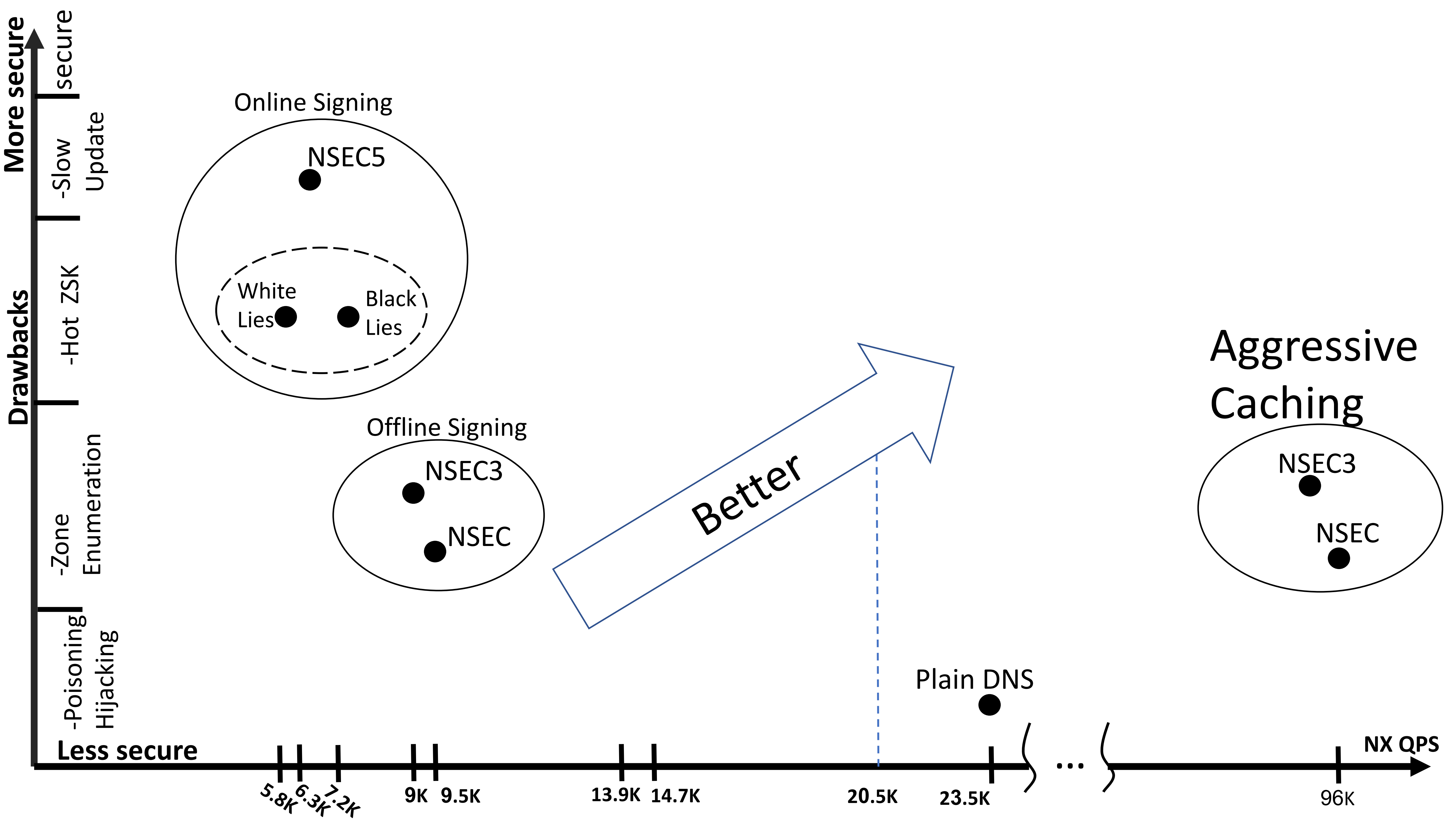

More secure
Drawbacks
secure
-Slow Update
-Hot ZSK
-Zone Enumeration
-Poisoning Hijacking
Less secure
Plain DNS
NX QPS
5.8K
6.3K
7.2K
9K
9.5K
13.9K
14.7K
20.5K
23.5K
96K

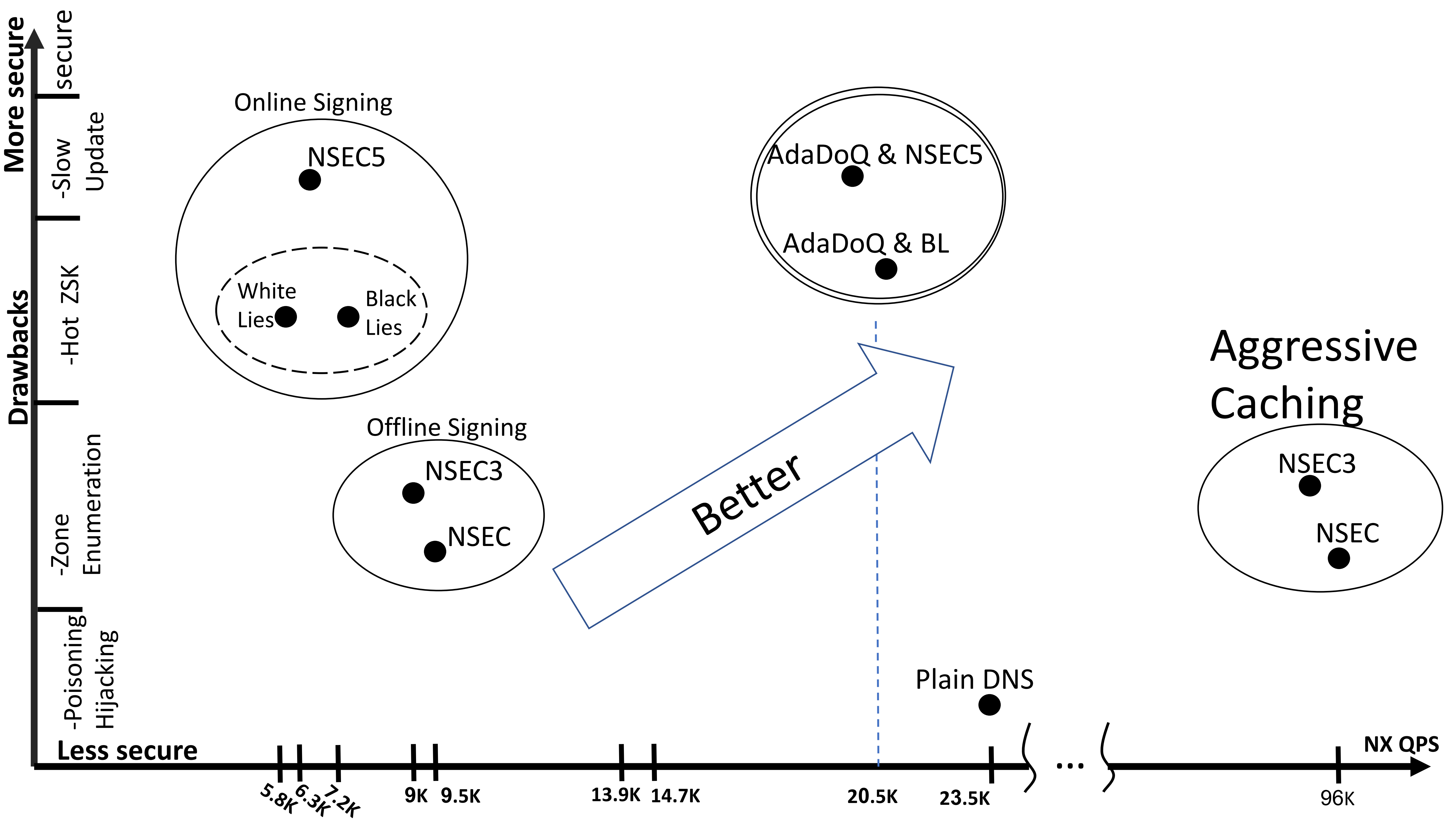

More secure
secure
-Slow
Update
-Hot ZSK
Drawbacks
-Zone
Enumeration
-Poisoning
Hijacking
Less secure
NSEC3
NSEC
Plain DNS
NX QPS
5.8K
6.3K
7.2K
9K
9.5K
13.9K
14.7K
20.5K
23.5K
96K


More secure
Drawbacks
secure
-Slow Update
-Hot ZSK
-Zone Enumeration
-Poisoning Hijacking
Less secure
NSEC3
NSEC
Better
Aggressive Caching
NSEC3
NSEC
Plain DNS
NX QPS
5.8K
6.3K
7.2K
9K
9.5K
13.9K
14.7K
20.5K
23.5K
...
96K

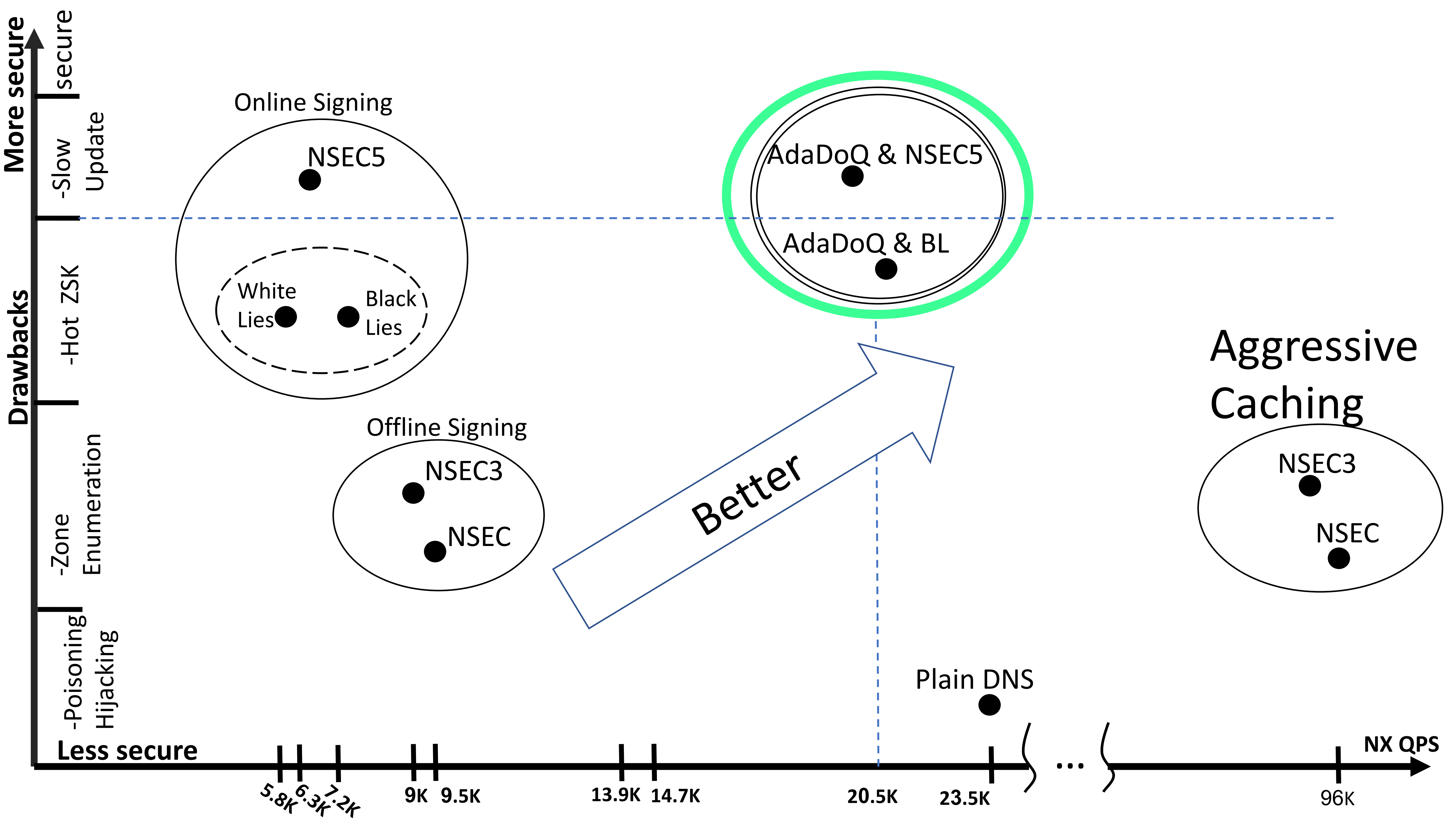


More secure
Drawbacks
Less secure
secure
-Slow Update
-Hot ZSK
-Zone Enumeration
-Poisoning Hijacking
NSEC3
NSEC
Better
Aggressive Caching
NSEC3
NSEC
Plain DNS
5.8K
6.3K
7.2K
9K
9.5K
13.9K
14.7K
20.5K
23.5K
...
96K
NX QPS


More secure
Drawbacks
Less secure
secure
-Slow Update
-Hot ZSK
-Zone Enumeration
-Poisoning Hijacking
Online Signing
NSEC5
White Lies
Black Lies
Offline Signing
NSEC3
NSEC
Better
Aggressive Caching
NSEC3
NSEC
Plain DNS
NX QPS
5.8K
6.3K
7.2K
9K
9.5K
13.9K
14.7K
20.5K
23.5K
...
96K



More secure
Drawbacks
secure
-Slow Update
-Hot ZSK
-Zone Enumeration
-Poisoning Hijacking
Less secure
Online Signing
NSEC5
White Lies
Black Lies
Offline Signing
NSEC3
NSEC
Better
AdaDoQ & NSEC5
AdaDoQ & BL
Aggressive Caching
NSEC3
NSEC
Plain DNS
NX QPS
5.8K
6.3K
7.2K
9K
9.5K
13.9K
14.7K
20.5K
23.5K
...
96K



More secure
Drawbacks
secure
-Slow Update
-Hot ZSK
-Zone Enumeration
-Poisoning Hijacking
Less secure
Online Signing
NSEC5
White Lies
Black Lies
Offline Signing
NSEC3
NSEC
AdaDoQ & NSEC5
AdaDoQ & BL
Better
Aggressive Caching
NSEC3
NSEC
Plain DNS
NX QPS
5.8K
6.3K
7.2K
9K
9.5K
13.9K
14.7K
20.5K
23.5K
...
96K

Conclusions

- DNSSEC degrades DNS performance
  - Make NXDOMAIN attacks worse (DDoS amplification)
- AdaDoQ – Hybrid Solution
  - Light and fast connections
  - One time encryption overheads
  - No Security Compromises
  - No Zone Walking
  - Close to Plain DNS throughput
  - No Scalability Issues

Questions?