Elliptic Curves to the rescue:

tackling availability issues and attack potential in DNSSEC

UNIVERSITY OF TWENTE.

SURF NET

Introduction

- DNSSEC deployment has taken off, but there are still operational issues:
  - Fragmentation
  - Amplification
  - Complex key management

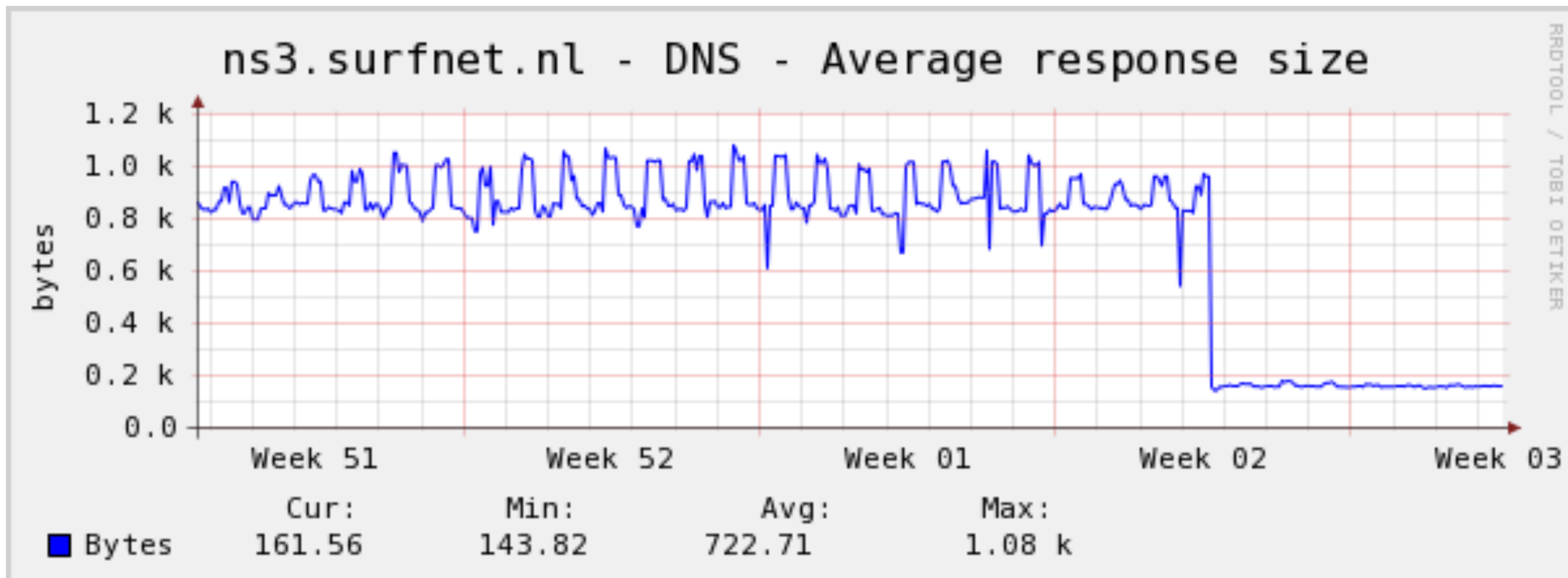
Fragmentation

- Well known problem; up to 10% of resolvers may not be able to receive fragmented responses*
- Solutions available:
    - Configure **minimal responses**
    - Better fallback behaviour in resolver software
    - Stricter phrasing of RFC 6891 (EDNS0)

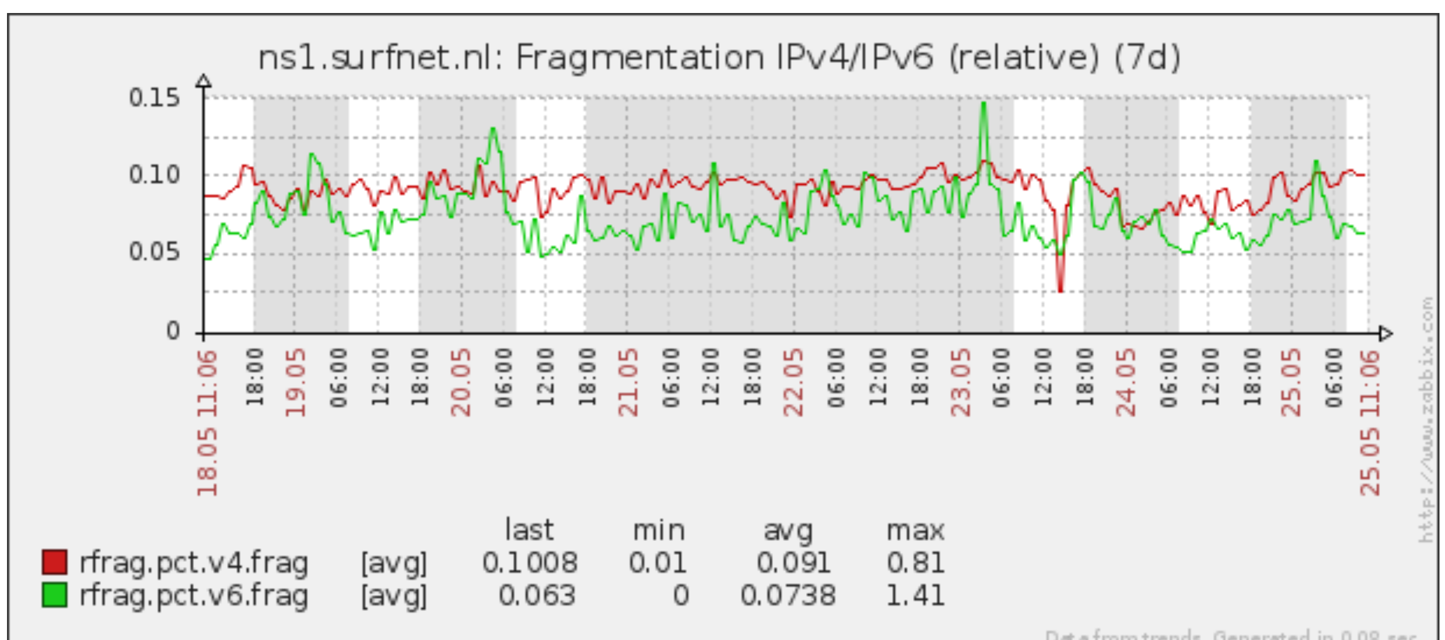
*Van den Broek, J., Van Rijswijk-Deij, R., Pras, A., Sperotto, A., “DNSSEC Meets Real World: Dealing with Unreachability Caused by Fragmentation”, IEEE Communications Magazine, volume 52, issue 4 (2014).

Fragmentation

- Setting **minimal responses** pays off:

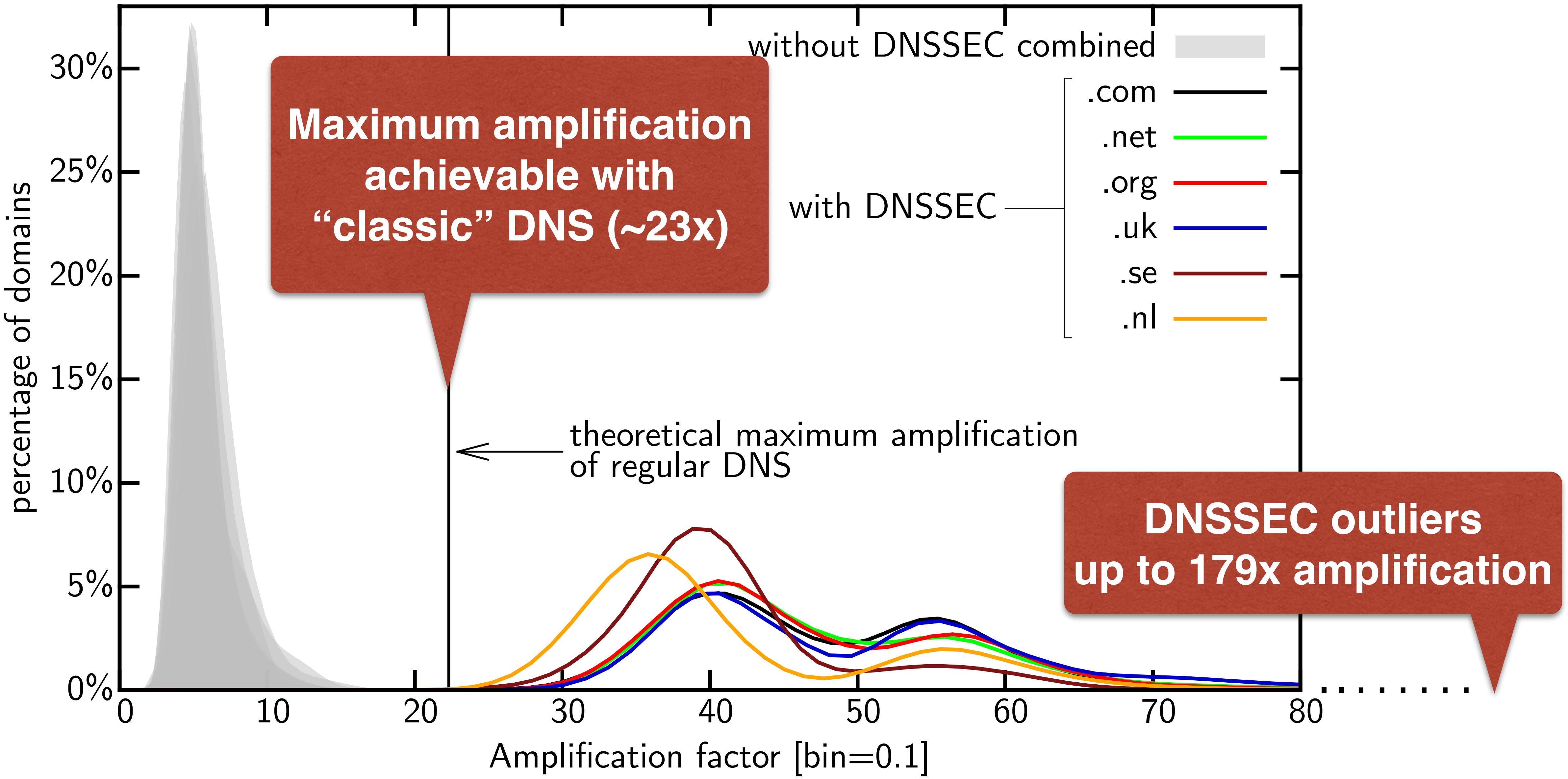


- But fragmentation still occurs!



Amplification

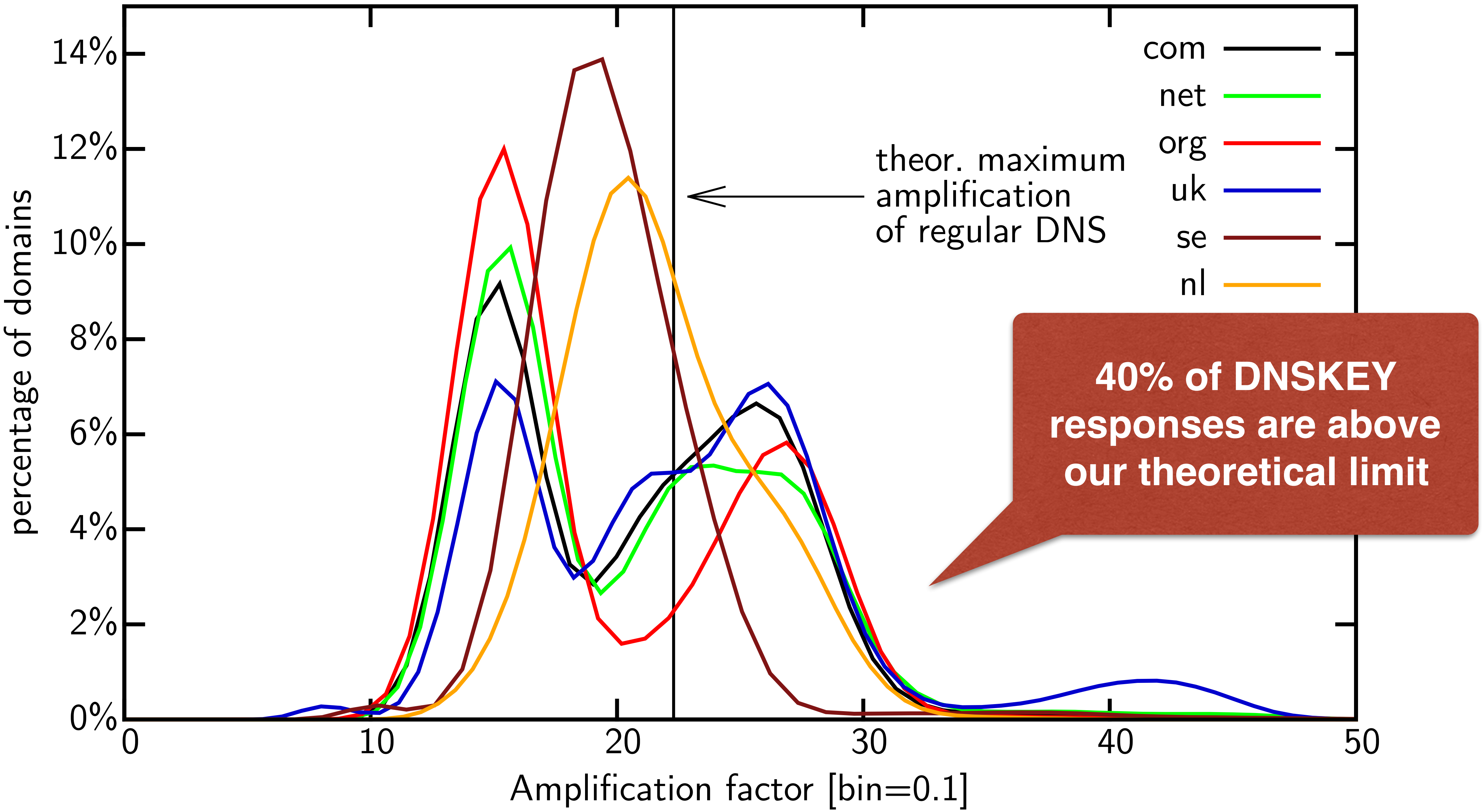
- DNSSEC is a potent amplifier*



* Van Rijswijk-Deij, R., Sperotto, A., & Pras, A. (2014). DNSSEC and its potential for DDoS attacks. In Proceedings of ACM IMC 2014. Vancouver, BC, Canada: ACM Press

Amplification

- While ANY could be suppressed, DNSKEY cannot!



Root cause: RSA

- RSA keys are large
  - 1024-bit —> 128 byte signatures
    ±132 bytes DNSKEY records
  - 2048-bit —> 256 byte signatures
    ±260 bytes DNSKEY records
- Also: striking a balance between signature size and key strength means RSA prevents a switch to simpler key management mechanisms*

*don't have time to explain in detail, see paper

Elliptic Curves to the rescue

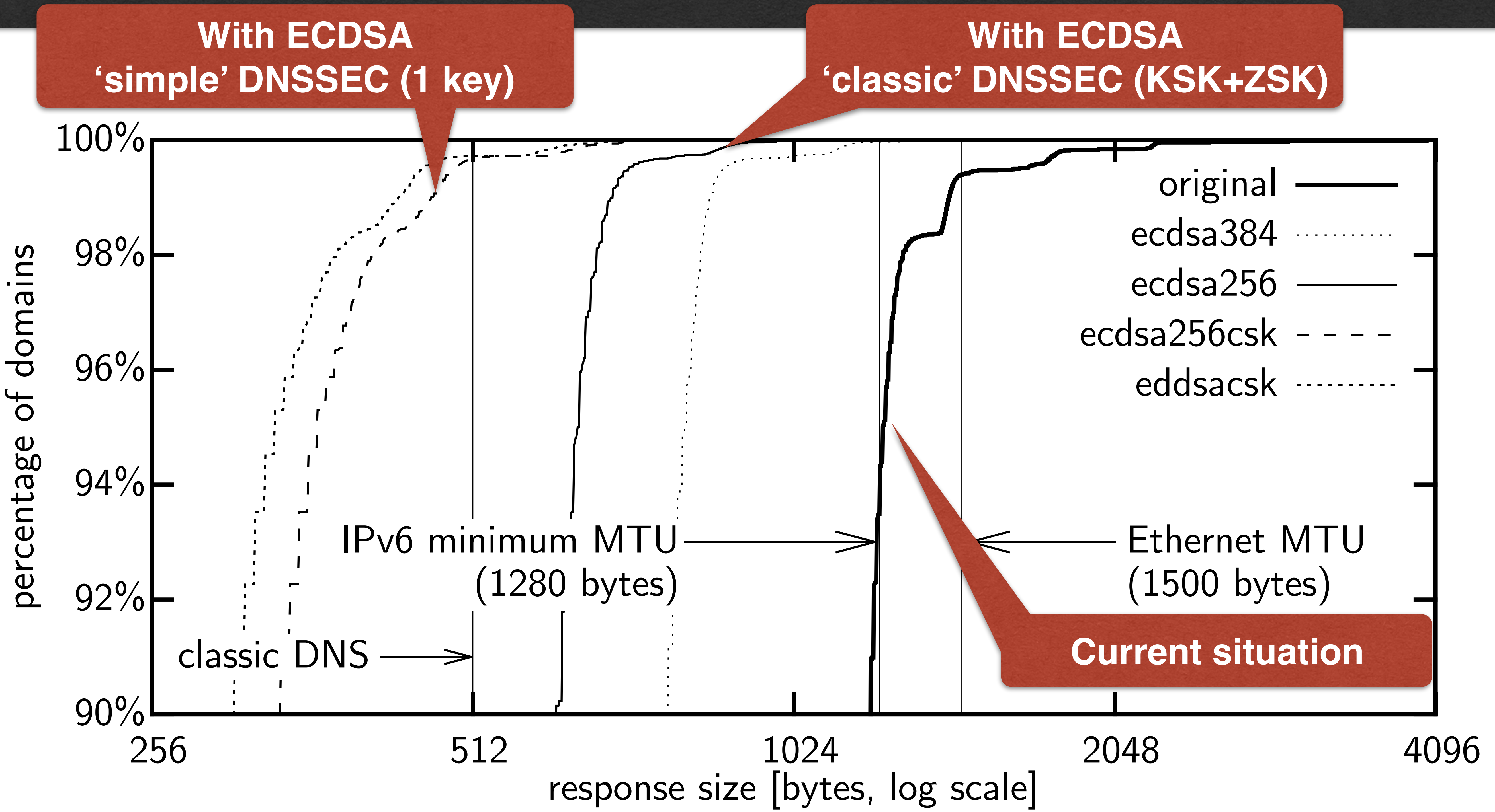
- ECC has much smaller keys and signatures with equivalent or better key strength
    - **ECC with 256-bit group ≈ RSA 3072-bit**
- **ECDSA P-256 and P-384 are standardised** for use in DNSSEC in **RFC 6605** (2012)
    - Still used very little in practice, **98.2% of signed .com domains use RSA**
    - But there is a lot of buzz around it (e.g. **CloudFlare, the 1.8% in .com** that uses ECDSA)
- EdDSA based schemes have draft RFCs (Ondřej Surý)

Measuring ECC impact

- We performed a measurement study to quantify the impact of switching to ECC on fragmentation and amplification
- Study looks at all signed .com, .net and .org domains
- Studies ECC scenarios:

implementation choice	ecdsa384	ecdsa256	ecdsa384csk	ecdsa256csk	eddsasplit	eddsacsk
ECDSA vs. EdDSA	ECDSA	ECDSA	ECDSA	ECDSA	EdDSA	EdDSA
Curve	P-384	P-256	P-384	P-256	Ed25519	Ed25519
KSK/ZSK vs. CSK	KSK/ZSK	KSK/ZSK	CSK	CSK	KSK/ZSK	CSK
	most conservative		⟵	⟶		*most beneficial*

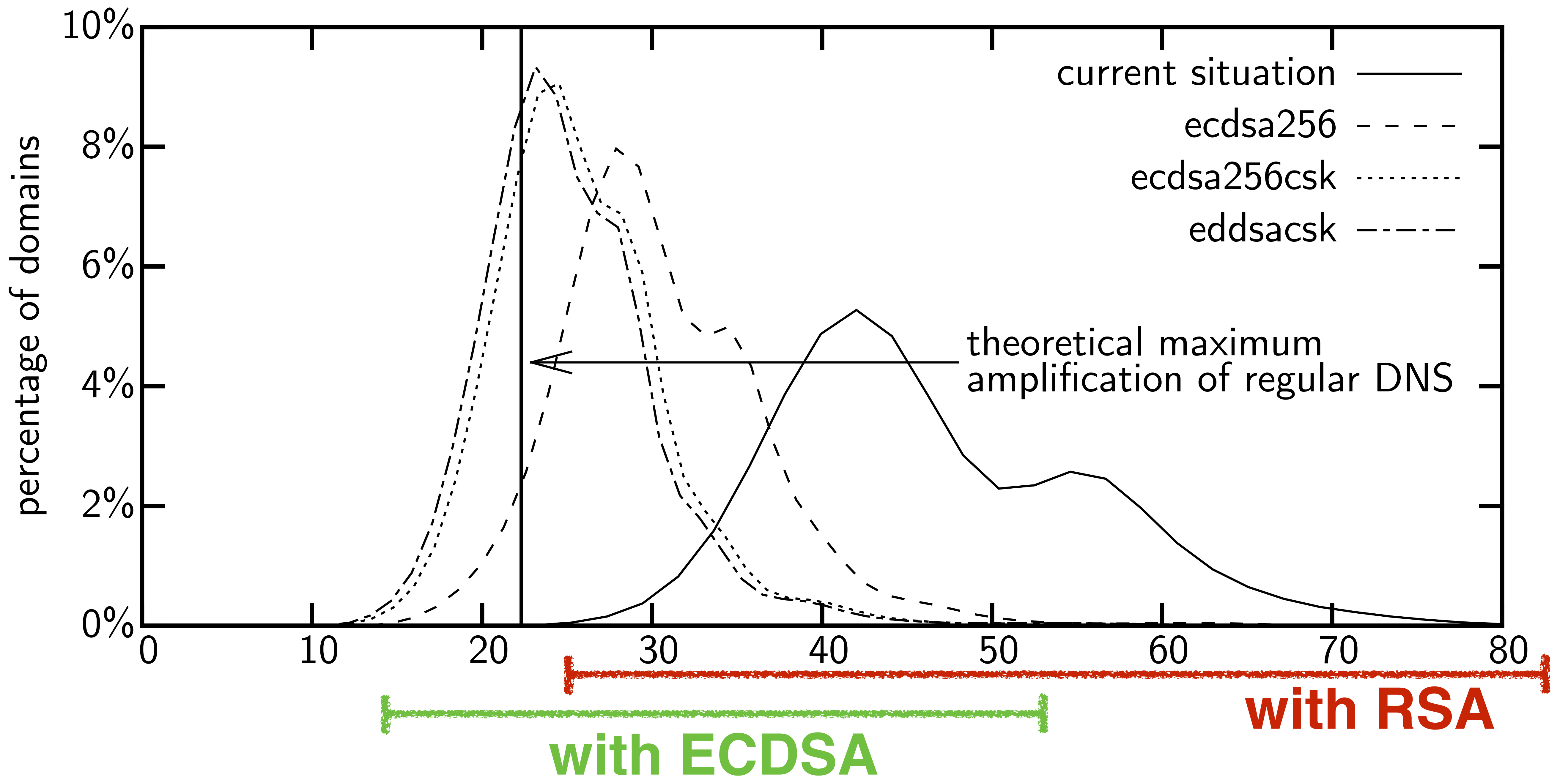
Impact on fragmentation



- DNSKEY response sizes dramatically reduced

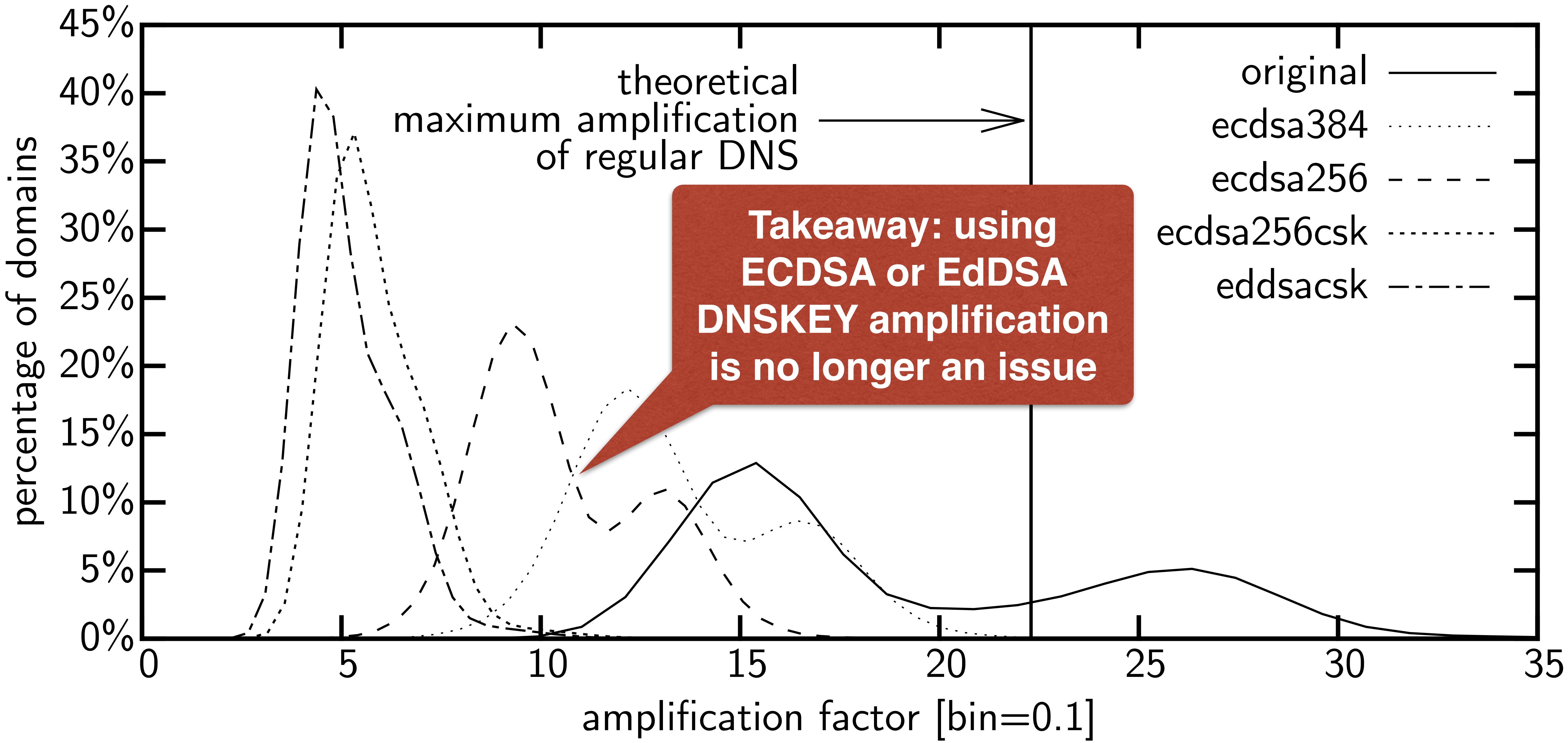
Impact on amplification

- ANY amplification dampened significantly:



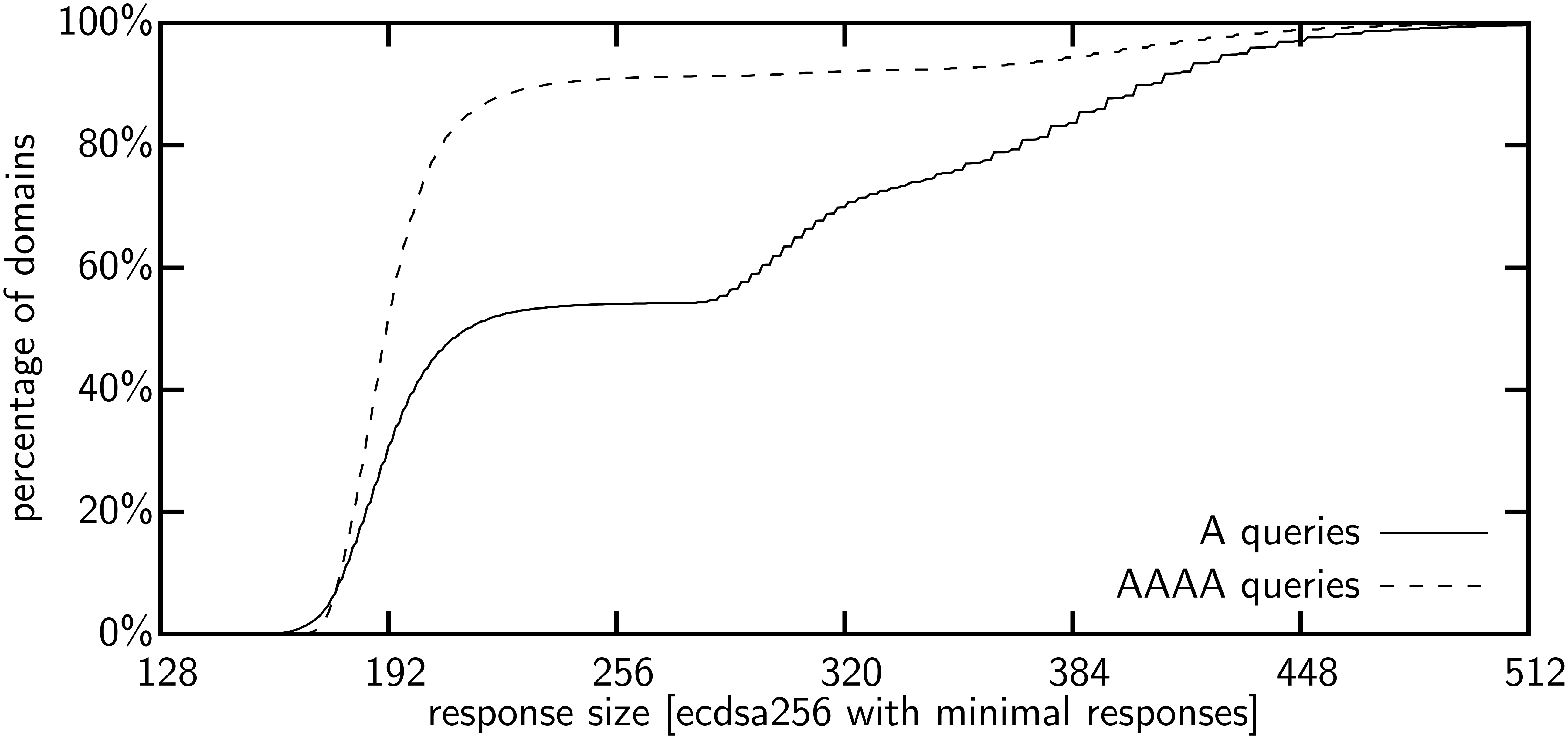
Impact on amplification

- DNSKEY amplification practically solved:



Back to 512-byte DNS?

- A and AAAA responses fit in classic DNS!



One little problem…

- Standardised ECC schemes (in DNSSEC) can be up to an order of magnitude slower when validating signatures —> **impact on DNS resolvers!**

		Compared to*			
		RSA		ECDSA	
ECC algorithm	OpenSSL version	1024	2048	P-256	P-384
ECDSA P-256	0.9.8zh	27.5	8.4	-	-
	1.0.1f	26.0	7.9	-	-
	1.0.2e	11.5	3.6	-	-
ECDSA P-384	0.9.8zh	57.7	17.6	-	-
	1.0.1f	77.6	23.4	-	-
	1.0.2e	87.3	27.2	-	-
Ed25519	(1.0.2e)†	7.9	2.5	0.7	0.1
Ed448	(1.0.2e)†	23.4	7.3	2.0	0.3

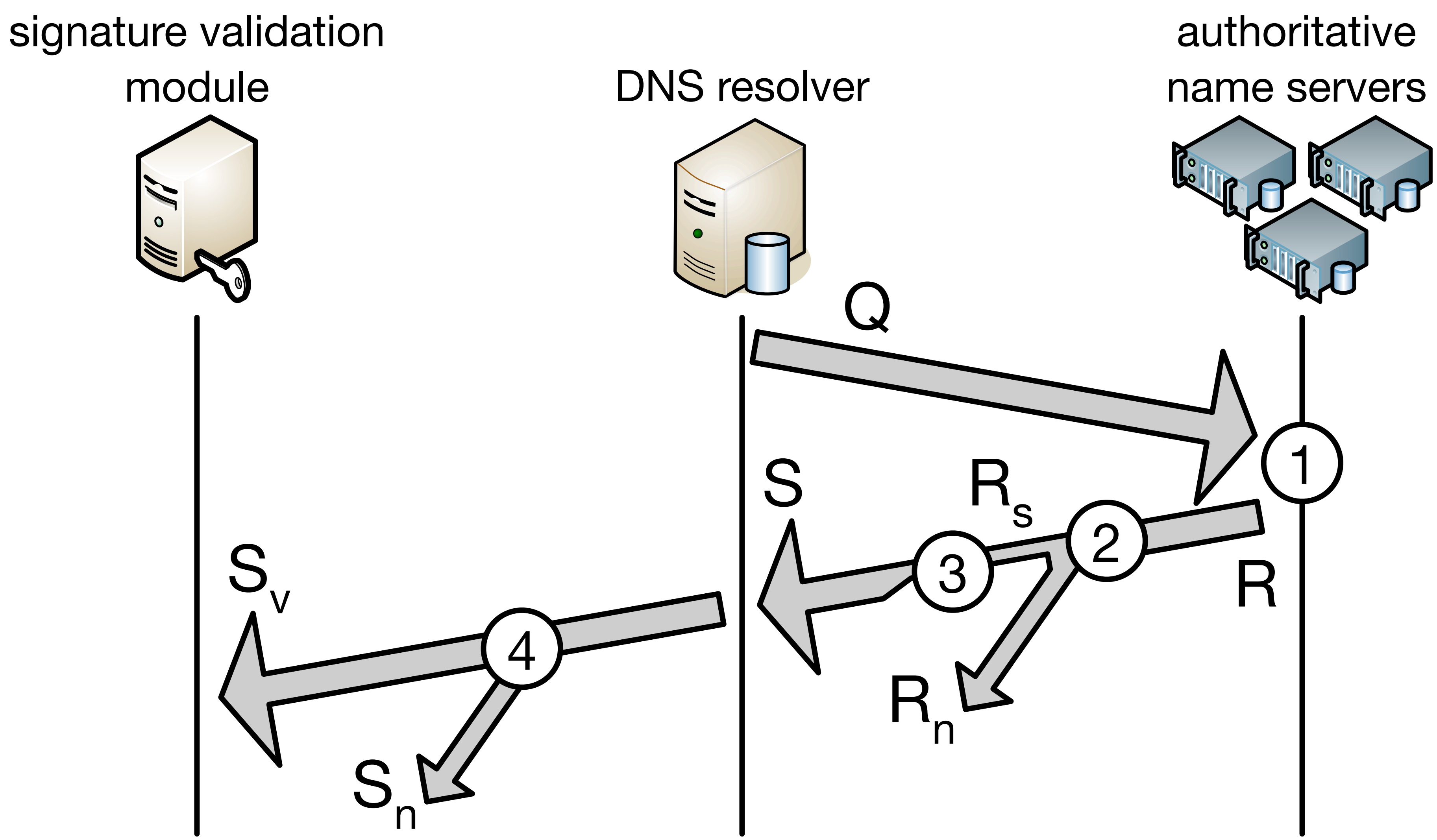
*the number means that the ECC algorithm is x times *slower*

†independent implementations compared to this OpenSSL version

Real-world impact?!

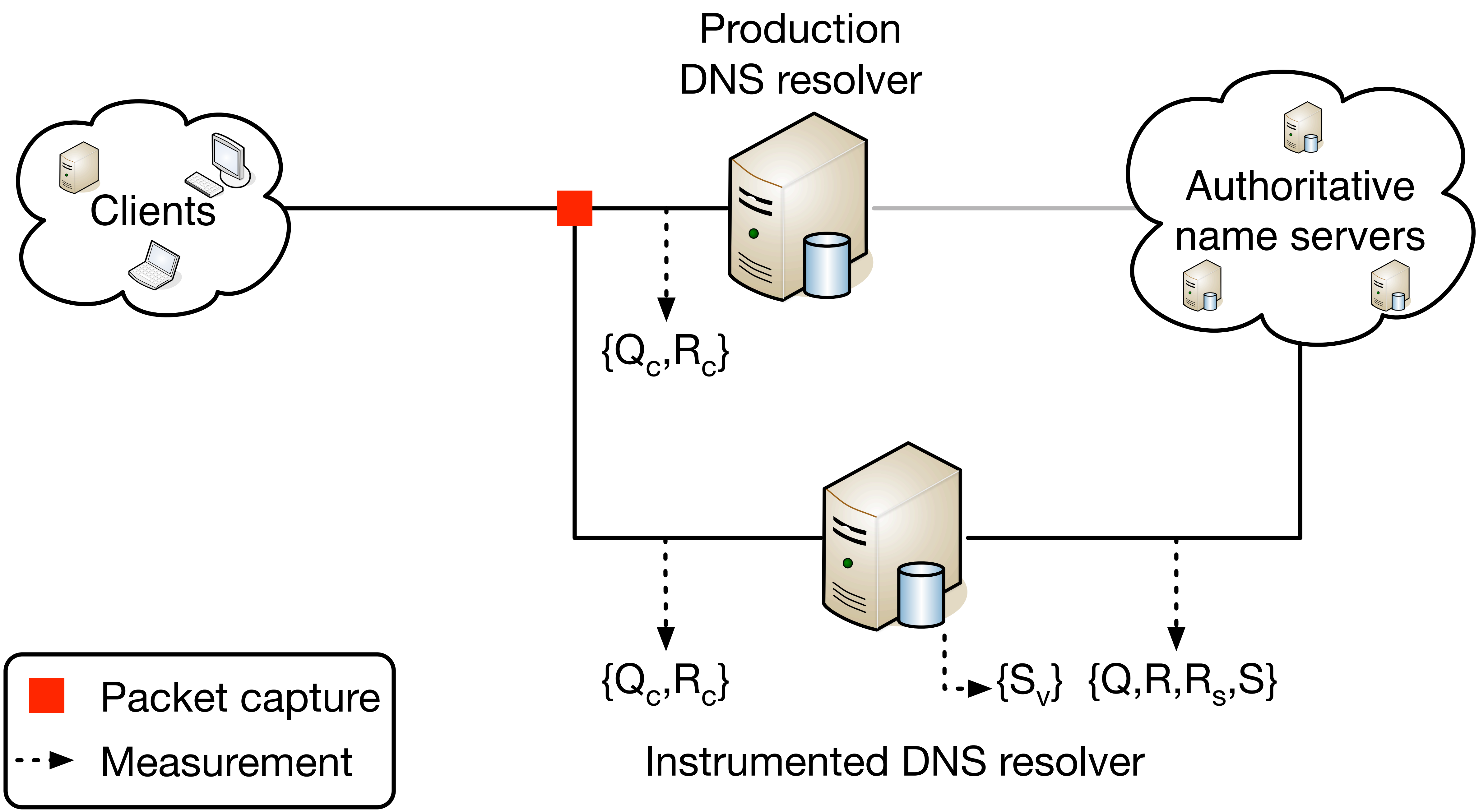
- We want to be sure deploying ECC DNS(SEC)-wide is not pushing the problem to the edges of the network (i.e. resolvers)
- So what would a switch mean for resolver CPU load?
- Let’s find out!

Resolver behaviour



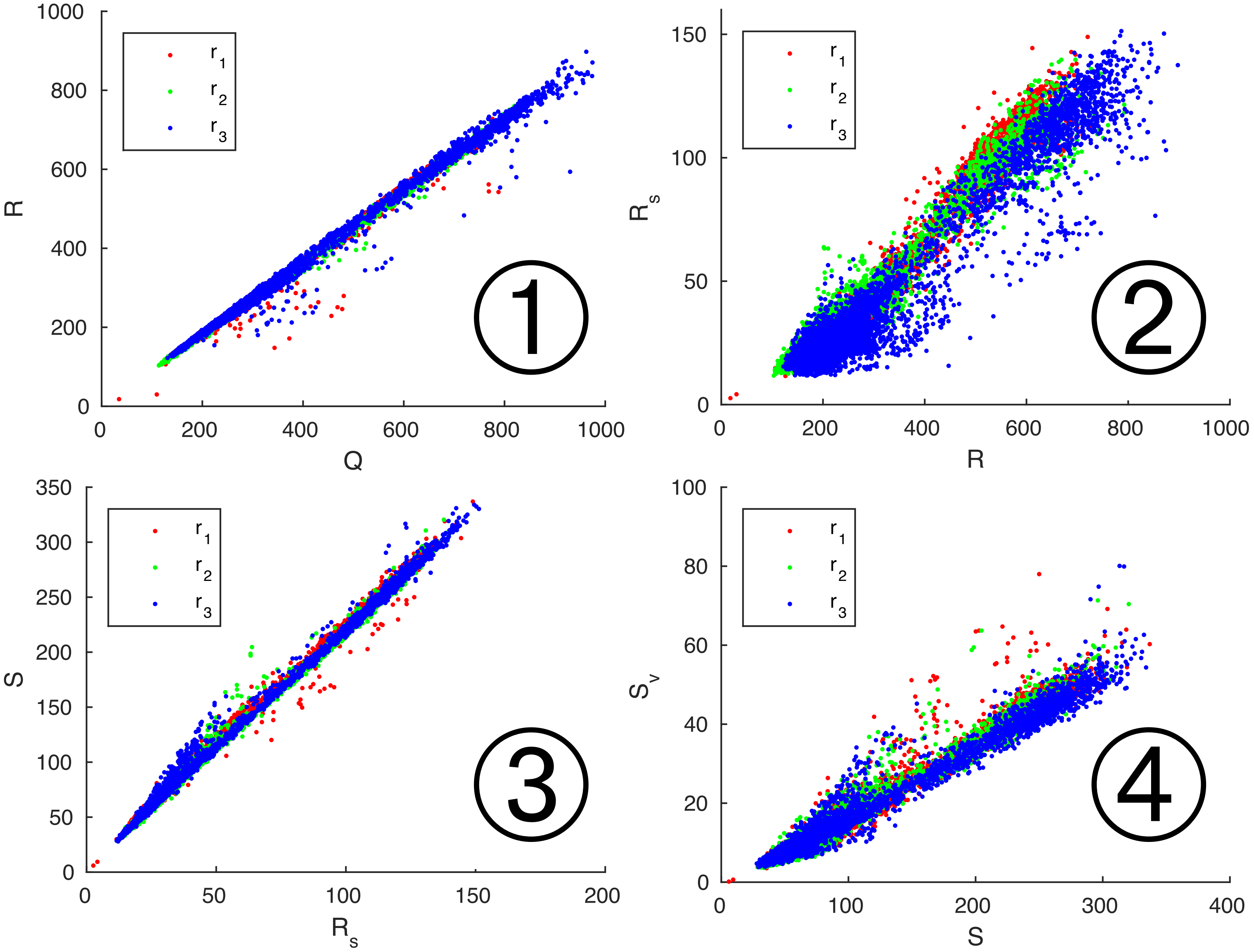
- Intuition: we can predict the number of signatures validations (S_v) based on the number of outgoing queries from a resolver (Q)

Measure using production traffic



- Instrumented versions of Unbound and BIND

Observed behaviour



- Intuition: *a linear model can predict S_v from Q*

Evaluating future scenarios

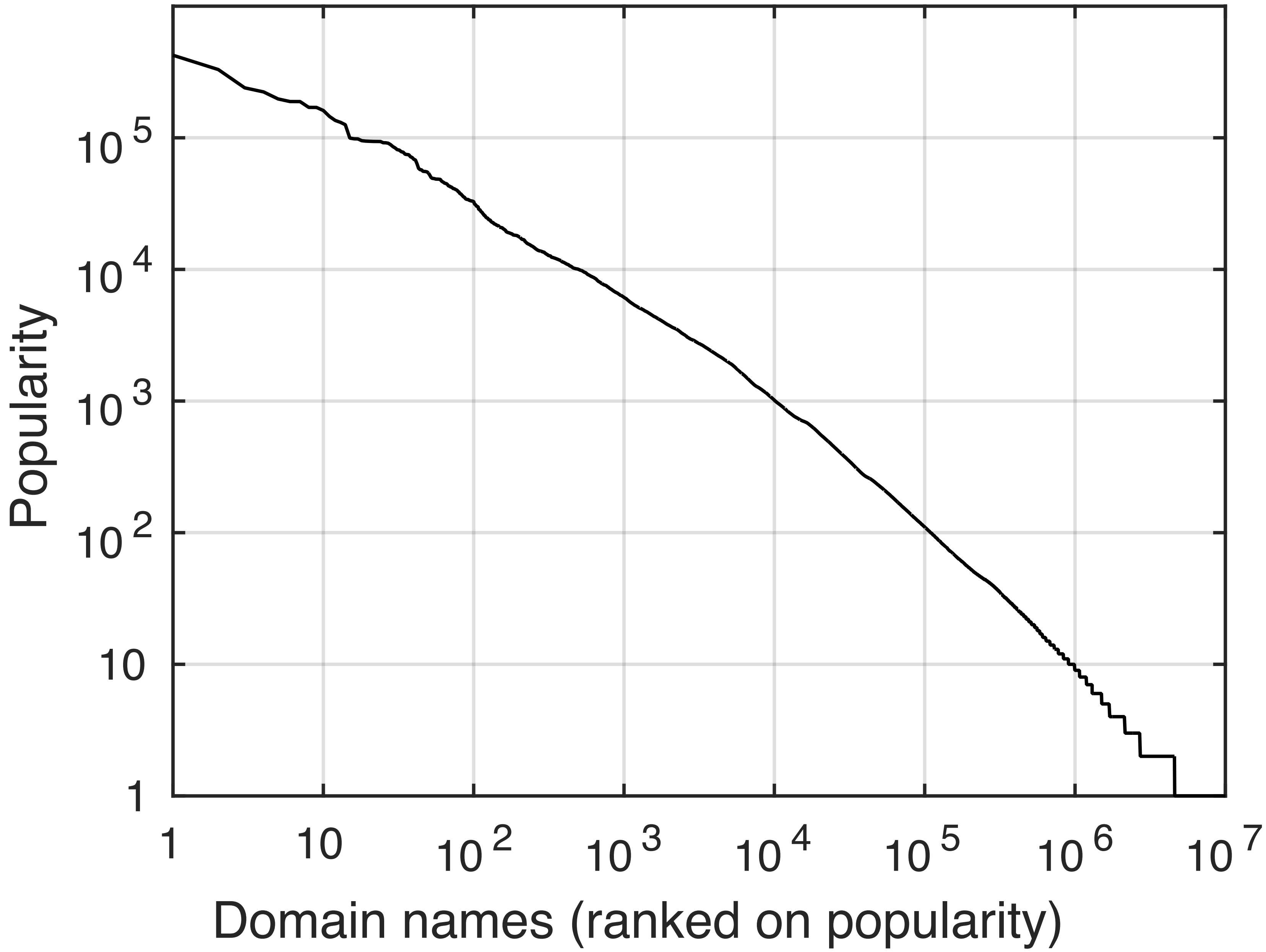
- Scenario 1:
  Current DNSSEC deployment switches to ECC overnight

  evaluation: requires ±150 validations per second for a busy* resolver, not a problem

- **Scenario 2:**
  Popular-domains-first growth to 100% DNSSEC deployment, everyone uses ECC

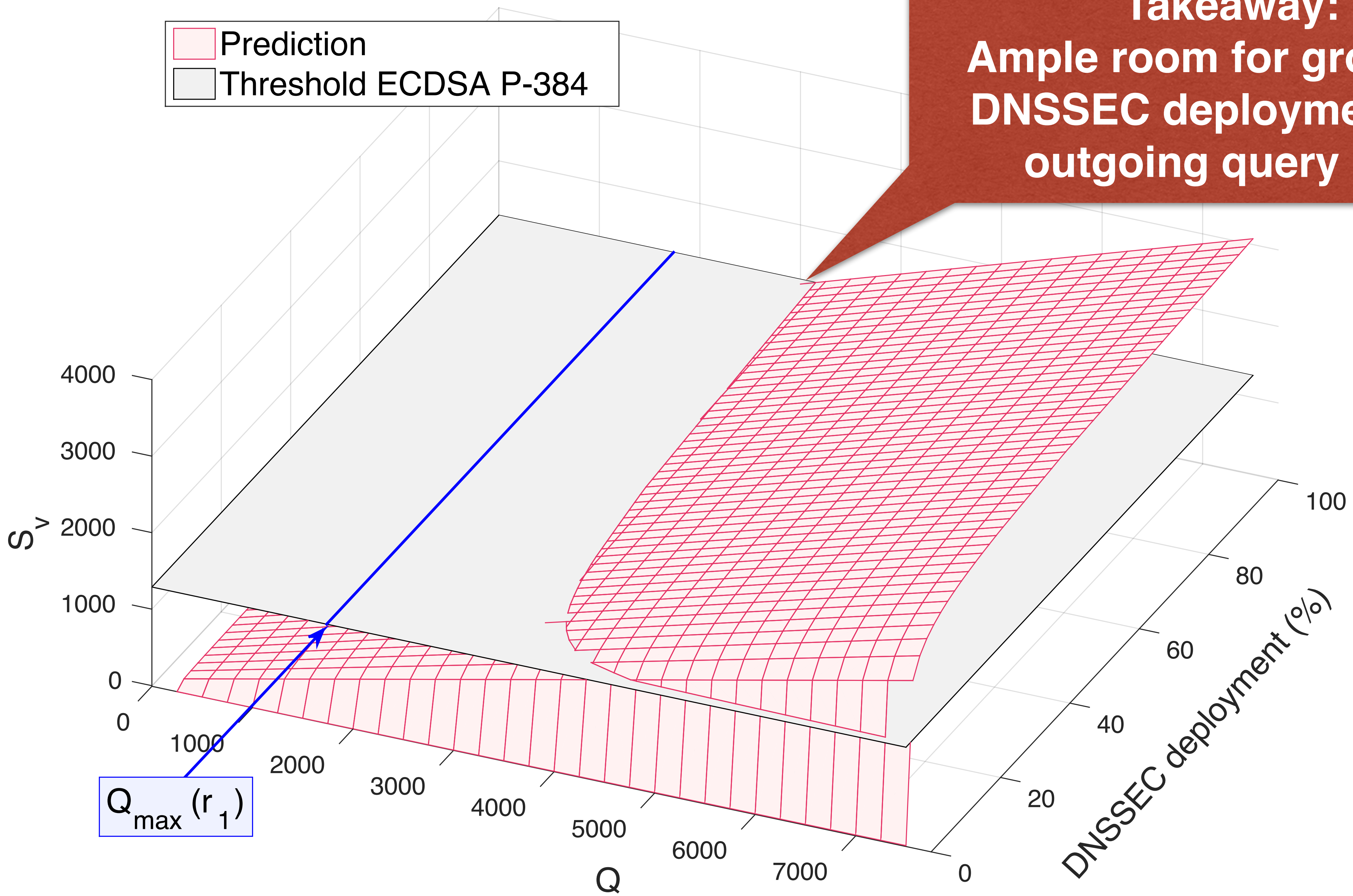
*our busiest resolver processes ~20k qps from clients

What is popular?



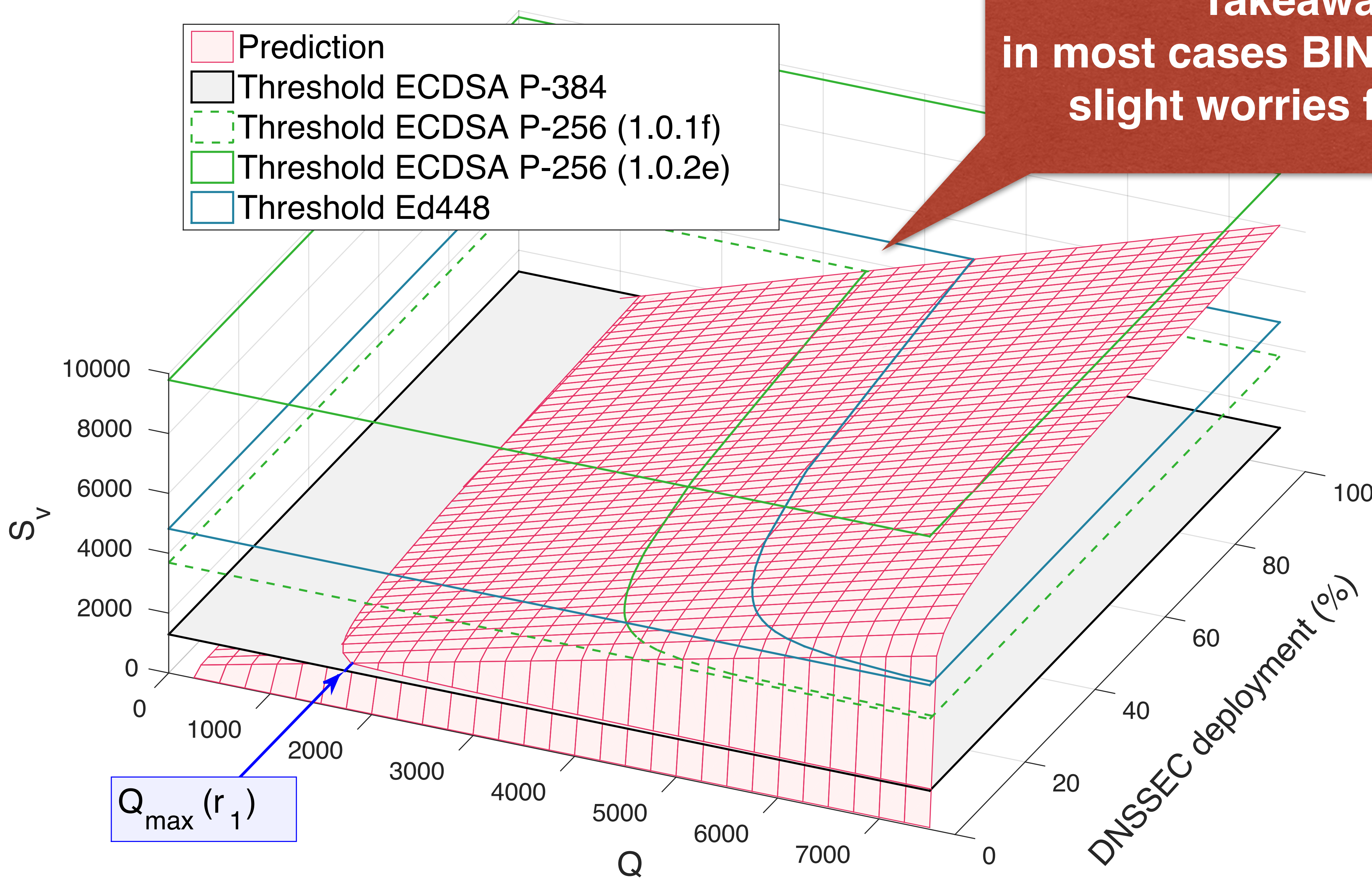
- "Classic" Internet distribution (Zipf, long-tail, …)

Scenario 2: Unbound



Takeaway:
Ample room for growth in DNSSEC deployment and outgoing query load

Scenario 2: BIND



Takeaway:
in most cases BIND will cope,
slight worries for P-384

Conclusions

- **Switching to ECC is highly beneficial** and tackles major issues in DNSSEC

- Combined with simpler key management it **could** even **bring “classic” 512-byte DNS back** into scope

- **Impact on resolvers is well within reason**

  - Improvements are being made (e.g. OpenSSL)

- Still **some open issues***, **but** these are **transient**

*resolver support for ECDSA
—> see work of Geoff Huston & George Michaelson

Recommendations

- **For DNSSEC signer operators:**
  - *Planning a new deployment?*
    Choose ECDSA P-256 as signing algorithm
  - *Existing deployment:*
    Consider **switch**ing **to ECDSA** (or even EdDSA) as part of your upgrade/replacement cycle (not trivial)
    (this is what we will be doing in 2017)
- **For DNS resolver operators:**
  - *Doing DNSSEC validation?*
    Check support for ECDSA, consider upgrading if not supported

Further reading

- DNSSEC Meets Real World: Dealing with Unreachability Caused by Fragmentation.
  IEEE Communications Magazine, 52 (April), 2014
  http://bit.ly/commag14-dnssec-frag


DNSSEC meets real world: dealing with unreachability caused by fragmentation

- DNSSEC and its potential for DDoS attacks
  Proceedings of ACM IMC 2014, Vancouver, BC, Canada
  http://bit.ly/imc14-dnssec


DNSSEC and Its Potential for DDoS Attacks

- Making the Case for Elliptic Curves in DNSSEC
  ACM Computer Communication Review (CCR), 45(5).
  http://bit.ly/ccr15-ecdsa


Making the Case for Elliptic Curves in DNSSEC

- SURFnet DNSSEC blog (we will be updating this when we migrate our signer infrastructure to ECDSA)
  http://dnssec.surfnet.nl/

- Internet Society Deploy 360 Programme, DNSSEC
  http://www.internetsociety.org/deploy360/dnssec/

Internet Society | Deploy360 Programme

Thank you for your attention!
Questions?

acknowledgement: **thanks to Kaspar Hageman for his M.Sc. work on quantifying the impact of ECC on validating DNS resolvers**

nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil

roland.vanrijswijk@surfnet.nl
r.m.vanrijswijk@utwente.nl

UNIVERSITY OF TWENTE.

SURF NET