Making the Case for Elliptic Curves in DNSSEC

an analysis of the impact of switching to ECC based on current DNSSEC deployments in .com, .net and .org

UNIVERSITY OF TWENTE.

SURF NET

Introduction

- DNSSEC deployment has taken off, but there are still operational issues
  - Fragmentation
  - Amplification
  - Complex key management
- Root cause of many of these problems: use of RSA
- ECDSA standardised in RFC 6605 (2012), but still sees very little use (but is discussed a lot!)

Fragmentation

- Well known problem; up to 10% of resolvers may not be able to receive fragmented responses*

- Solutions available:

  - Configure **minimal responses**

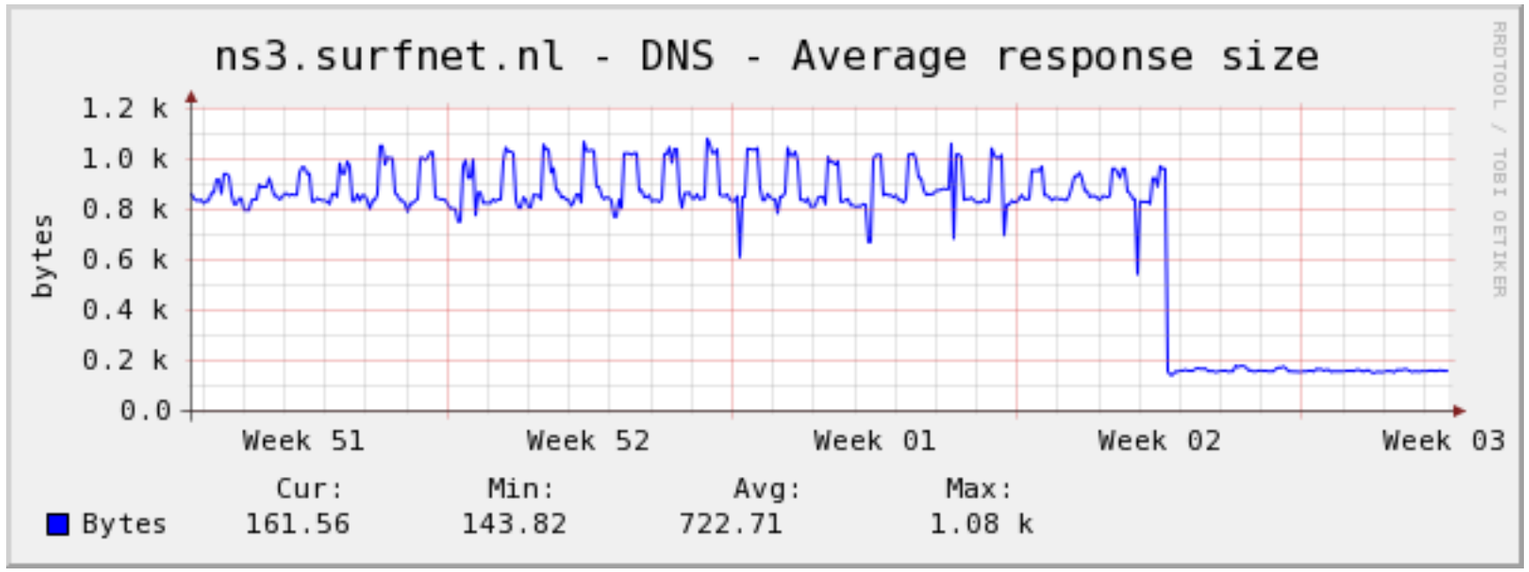
  - Better fallback behaviour in resolver software

  - Stricter phrasing of RFC 6891 (EDNS0)

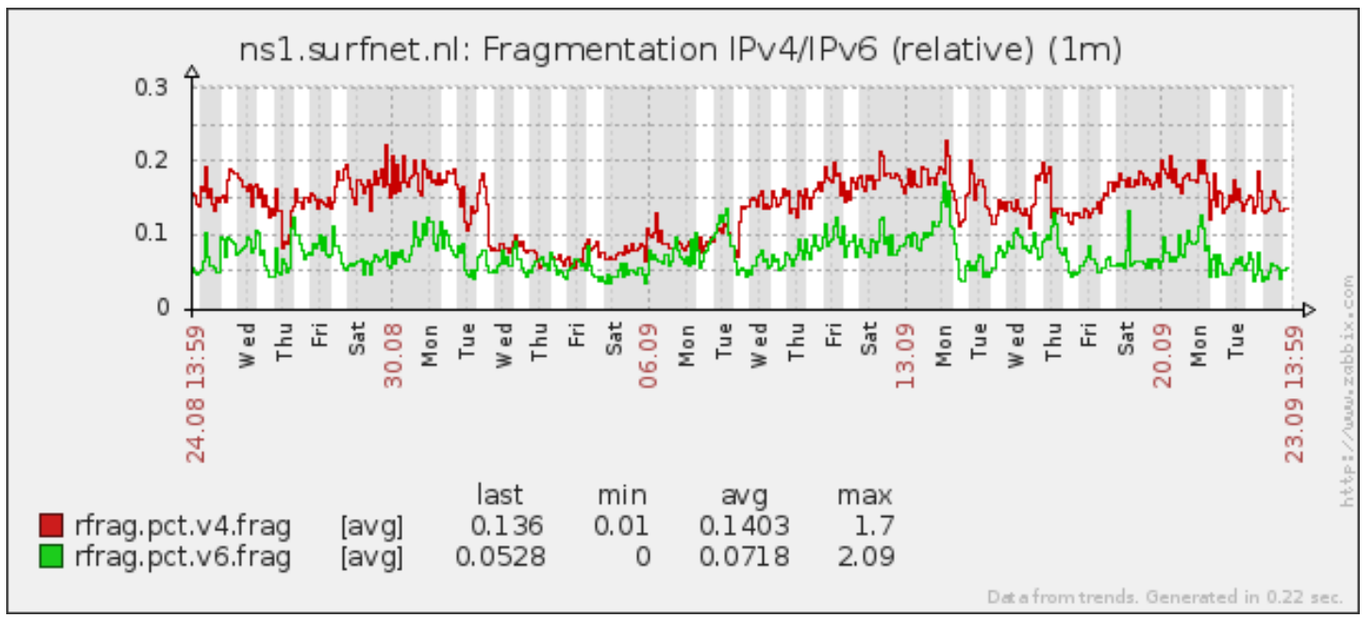
*Van den Broek, J., Van Rijswijk-Deij, R., Pras, A., Sperotto, A., “DNSSEC Meets Real World: Dealing with Unreachability Caused by Fragmentation”, IEEE Communications Magazine, volume 52, issue 4 (2014).

Fragmentation

- Setting **minimal responses** pays off:

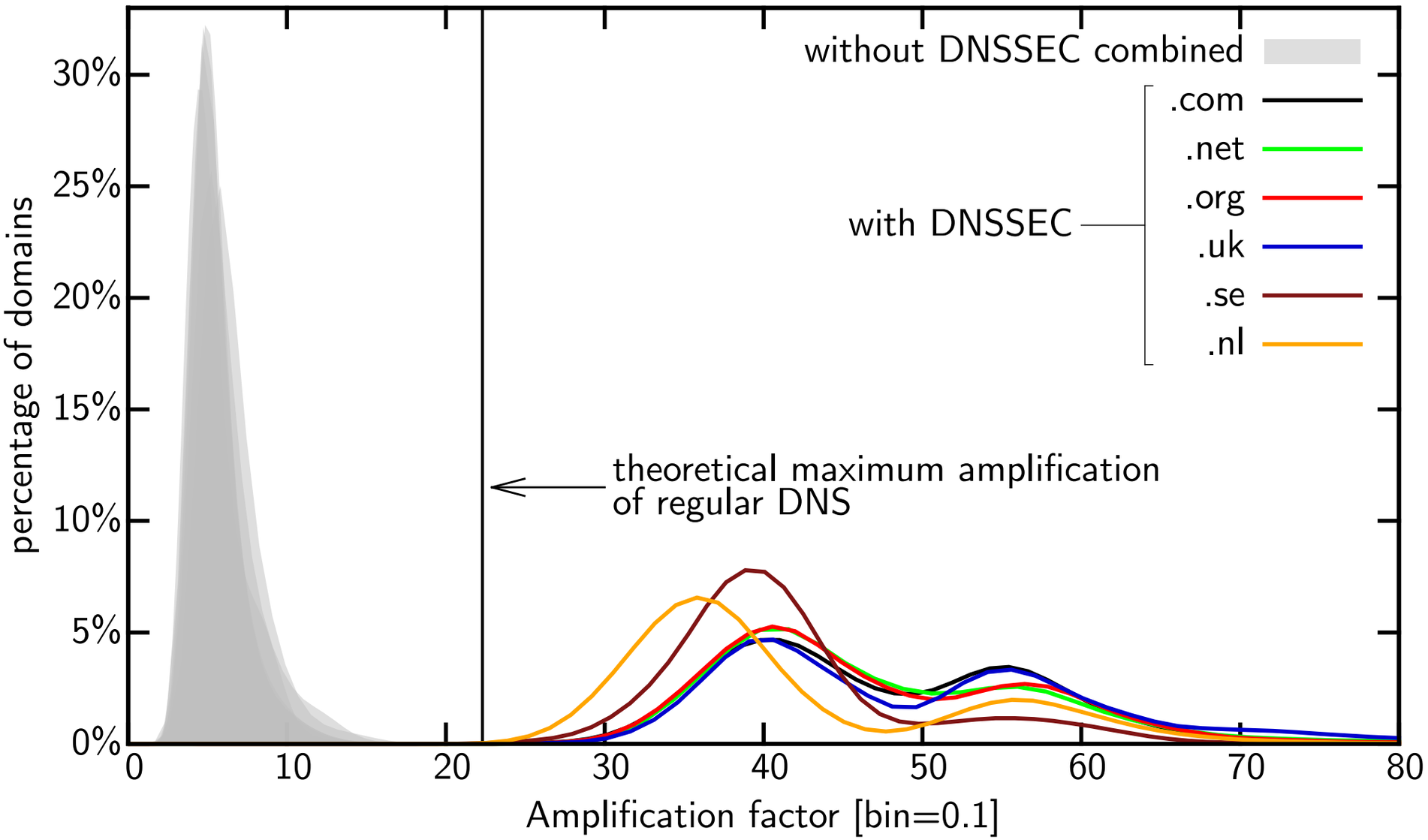


- But fragmentation still occurs!



Amplification

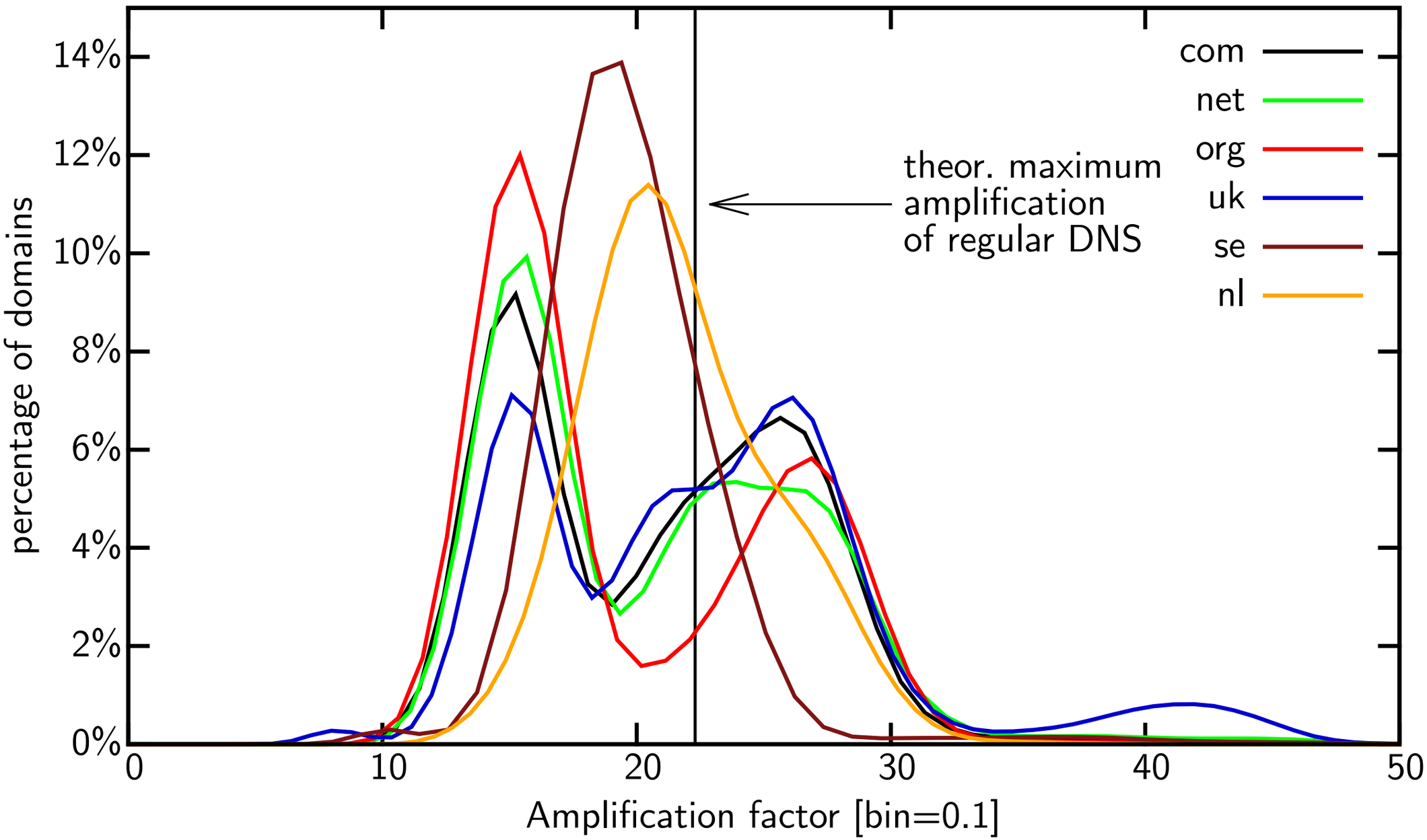
- DNSSEC is a potent amplifier*



* 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

ECC 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)
  - Used very little in practice, 99.99% of .com, .net and .org use RSA
  - But there is a lot of buzz around it (CloudFlare!)
- 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

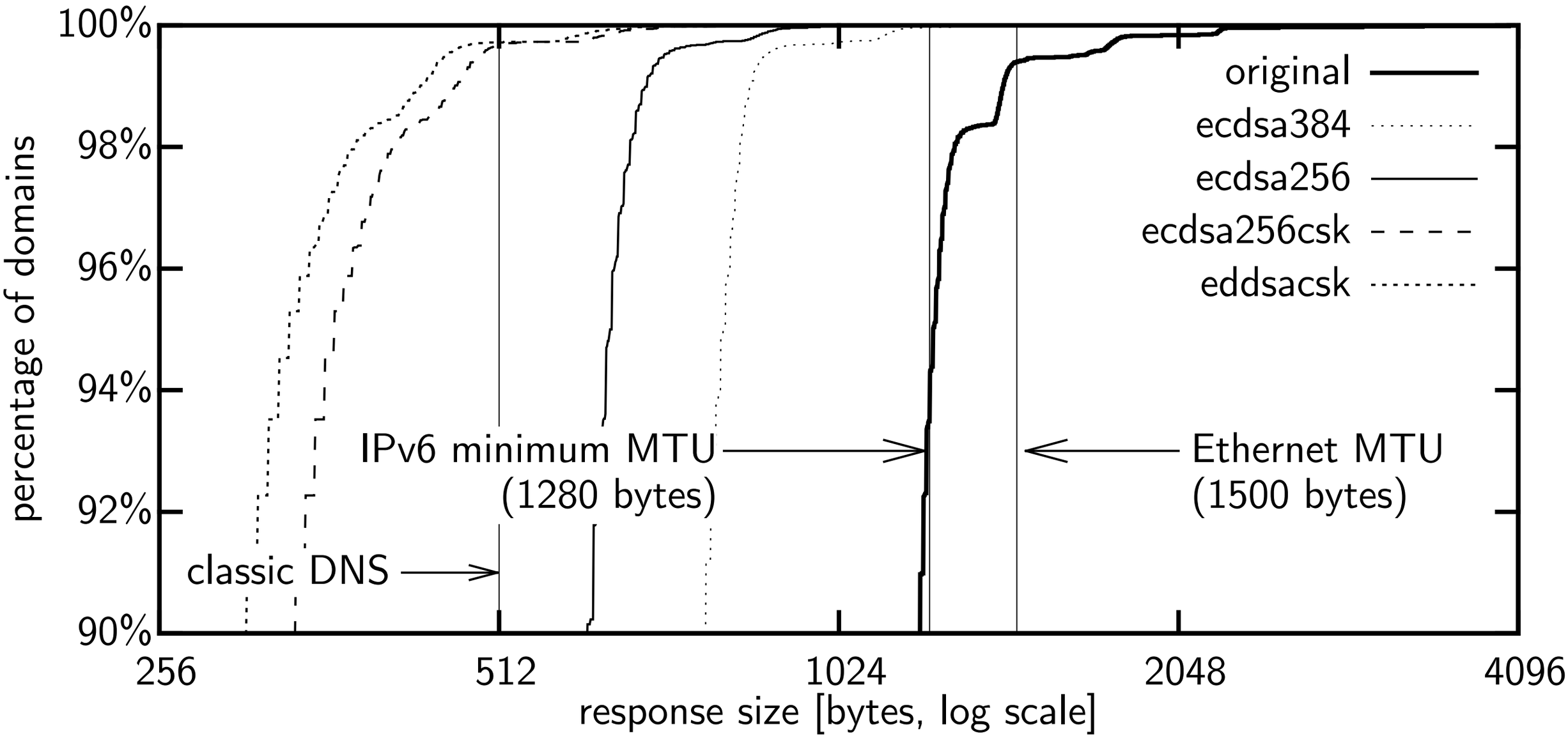
- Study looks at all signed .com, .net and .org domains

- 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*	

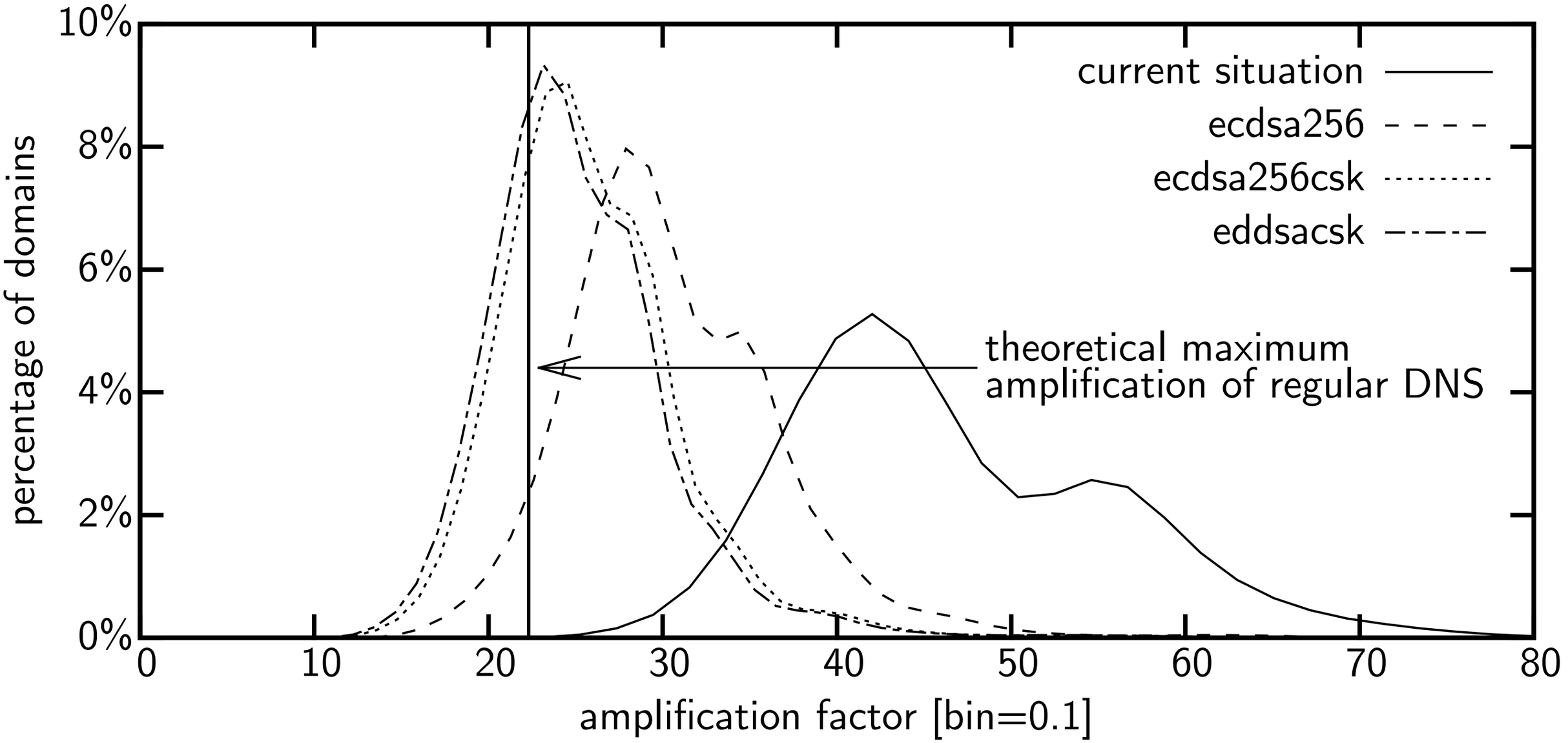
Impact on fragmentation

- DNSKEY response sizes dramatically reduced:



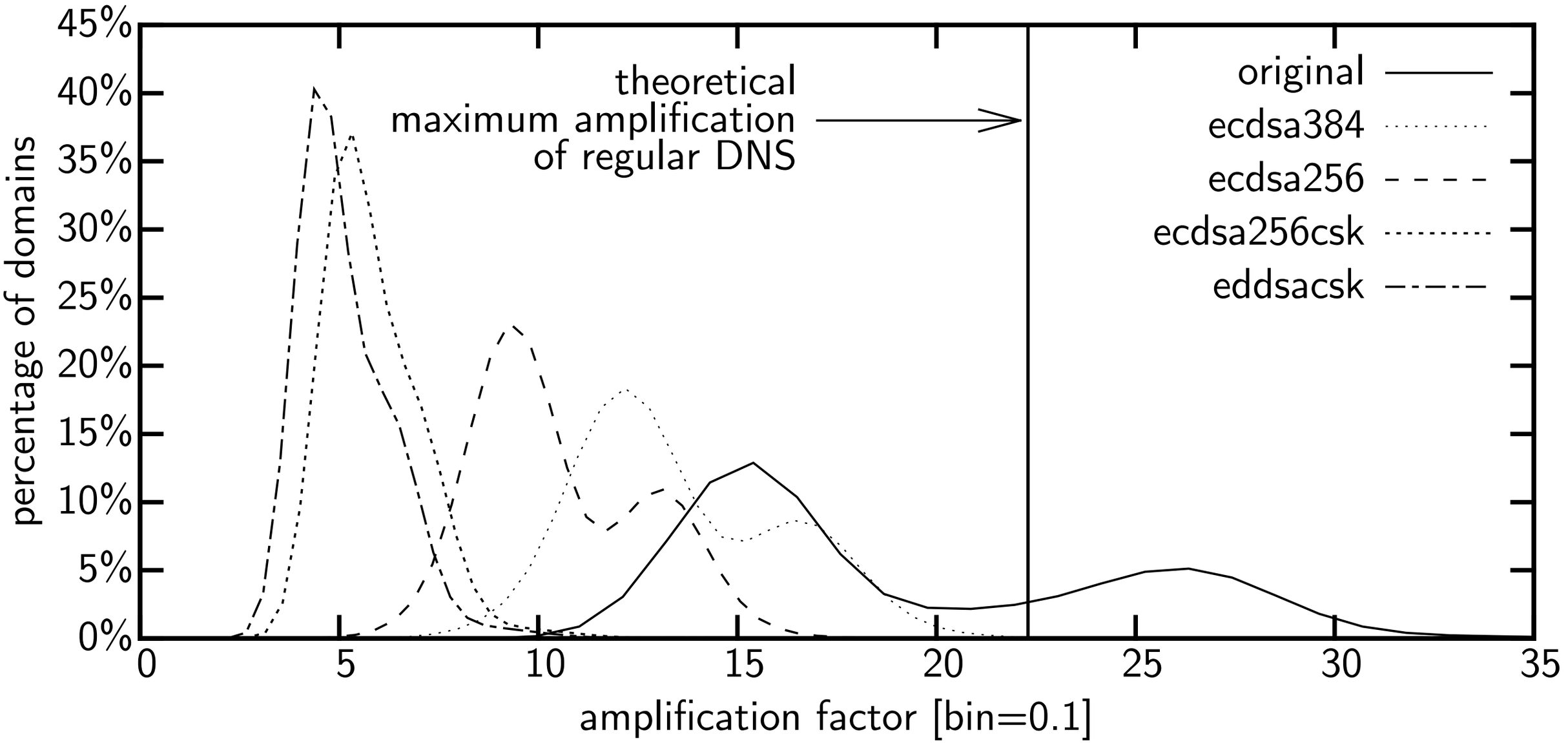
Impact on amplification

- ANY amplification dampened significantly:



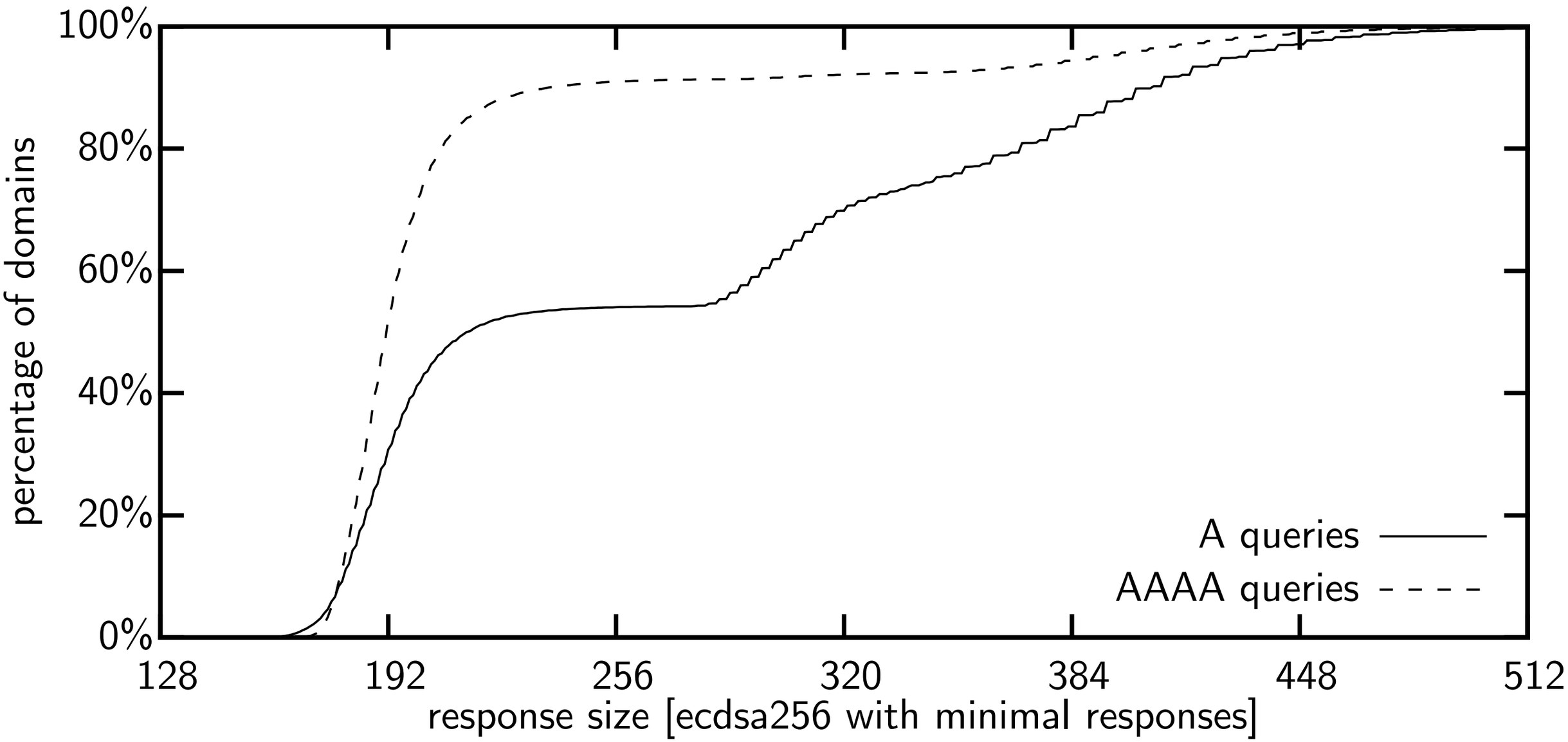
Impact on amplification

- DNSKEY amplification practically solved:



Back to 512-byte DNS?

- A and AAAA responses fit in classic DNS!



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 uncertain! ECC validation speeds are up to an order of magnitude slower than RSA
  - Improvements are being made (e.g. OpenSSL)
  - We are working on quantifying the impact of this

Further reading and future work

- For an in-depth discussion of this material, see our CCR paper*
- We are working on quantifying the impact of switching to ECC on resolvers (M.Sc.project finishing tomorrow, Oct. 22), expect another paper soon

Making the Case for Elliptic Curves in DNSSEC

Roland van Rijswijk-Deij
University of Twente and
SURFnet bv
r.m.vanrijswijk@utwente.nl

Anna Sperotto
University of Twente
a.sperotto@utwente.nl

Aiko Pras
University of Twente
a.pras@utwente.nl

ABSTRACT

The Domain Name System Security Extensions (DNSSEC) add authenticity and integrity to the DNS, improving its security. Unfortunately, DNSSEC is not without problems. DNSSEC adds digital signatures to the DNS, significantly increasing the size of DNS responses. This means DNSSEC is more susceptible to packet fragmentation and makes DNSSEC an attractive vector to abuse in amplification-based denial-of-service attacks. Additionally, key management policies are often complex. This makes DNSSEC fragile and leads to operational failures. In this paper, we argue that the choice for RSA as default cryptosystem in DNSSEC is a major factor in these three problems. Alternative cryptosystems, based on elliptic curve cryptography (ECDSA and EdDSA), exist but are rarely used in DNSSEC. We show that these are highly attractive for use in DNSSEC, although they also have disadvantages. To address these, we have initiated research that aims to investigate the viability of deploying ECC at a large scale in DNSSEC.

Keywords

DNS; DNSSEC; fragmentation; DDoS; amplification attack; elliptic curve cryptography; ECDSA; EdDSA

1. INTRODUCTION

The Domain Name System (DNS) performs a critical function on the Internet, translating human readable names into IP addresses. The DNS was never designed with security in mind, though. To address this, a major overhaul of the DNS is underway with the introduction of the DNS Security Extensions (DNSSEC). DNSSEC adds integrity and authenticity to the DNS, by digitally signing DNS data. These signatures are then validated by DNS resolvers to verify that data is authentic and has not been modified in transit.

While DNSSEC can improve the security of the Internet, uptake is still lacklustre. Less than 3% of domains worldwide deploy DNSSEC[1] and at best 13% of clients are protected by DNSSEC validation[2]. We argue that this is partly due to problems with DNSSEC as a technology. Three problems stand out. First, DNSSEC responses are larger and suffer more from IP fragmentation, which impacts availability [1]. Second, DNSSEC's larger responses can be abused for potent denial-of-service attacks [2]. Third, key management in DNSSEC is often complex, which may lead to mistakes that make domains unreachable. These issues raise the question if the benefits of DNSSEC outweigh the disadvantages.

We argue that one of the root causes of these problems is the choice of RSA as default signature algorithm for DNSSEC. RSA keys and signatures are large, compared to traditional DNS messages. There are alternatives, though, based on elliptic curve cryptography (ECC). ECC keys and signatures are much smaller, while their cryptographic strength is excellent. This is attractive for DNSSEC as it reduces response sizes, addressing the first two problems (fragmentation and amplification), and their cryptographic strength makes simpler key management feasible. One particular ECC-based scheme, ECDSA, was already standardised for use in DNSSEC in 2012, but is still rarely used in practice. Given the potential benefits, we argue that this should change. Therefore, we set out to build a case for a switchover to ECDSA and other elliptic curve signature schemes.

Our contribution – We quantify, based on real-world measurements, the effect of switching DNSSEC from RSA to ECC. Our results prove that ECC can mitigate the problems outlined above. But ECC also has disadvantages. We discuss these and have initiated research to study the Internet-scale effects of switching DNSSEC to ECC. This can help guide future standardisation in this area.

1.1 Related Work

The overhead of DNSSEC on the DNS was first studied by Ager et al. [3]. They mention ECC as an alternative to RSA, albeit not in much detail. We add to their work by providing a detailed up-to-date analysis.

Yang et al. [4] performed the first systematic analysis of DNSSEC as an Internet-scale deployment of public key cryptography. They examine cryptographic aspects as well as the complexities of incremental deployment, partial trust chains and key management. What they do not touch on, though, are problems with fragmentation and amplification that we argue are a direct result of choices related to cryptography.

Herzberg & Shulman [5], like us, discuss the problem of cryptographic algorithm choices in DNSSEC. They propose a protocol for DNS clients and servers to negotiate an optimal cipher suite. Their goal is to reduce the amount of cryptographic material that needs to be exchanged, in order to reduce DNS message sizes. While this reduces fragmentation and amplification, it does not reduce the complexity of key management. Rather, it further complicates the DNSSEC protocol. We choose a different path. Instead of introducing additional complexity, we build a case for a complete switch to elliptic curve cryptography in DNSSEC.

[1] http://www.isoc.org/deploy360/dnssec/statistics/
[2] http://stats.labs.apnic.net/dnssec/XA

*Van Rijswijk-Deij, R., Sperotto, A., & Pras, A. (2015). "Making the Case for Elliptic Curves in DNSSEC". ACM Computer Communication Review (CCR), 45(5).

Thank you for your attention!

Questions?

nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil

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

UNIVERSITY OF TWENTE.

SURF NET