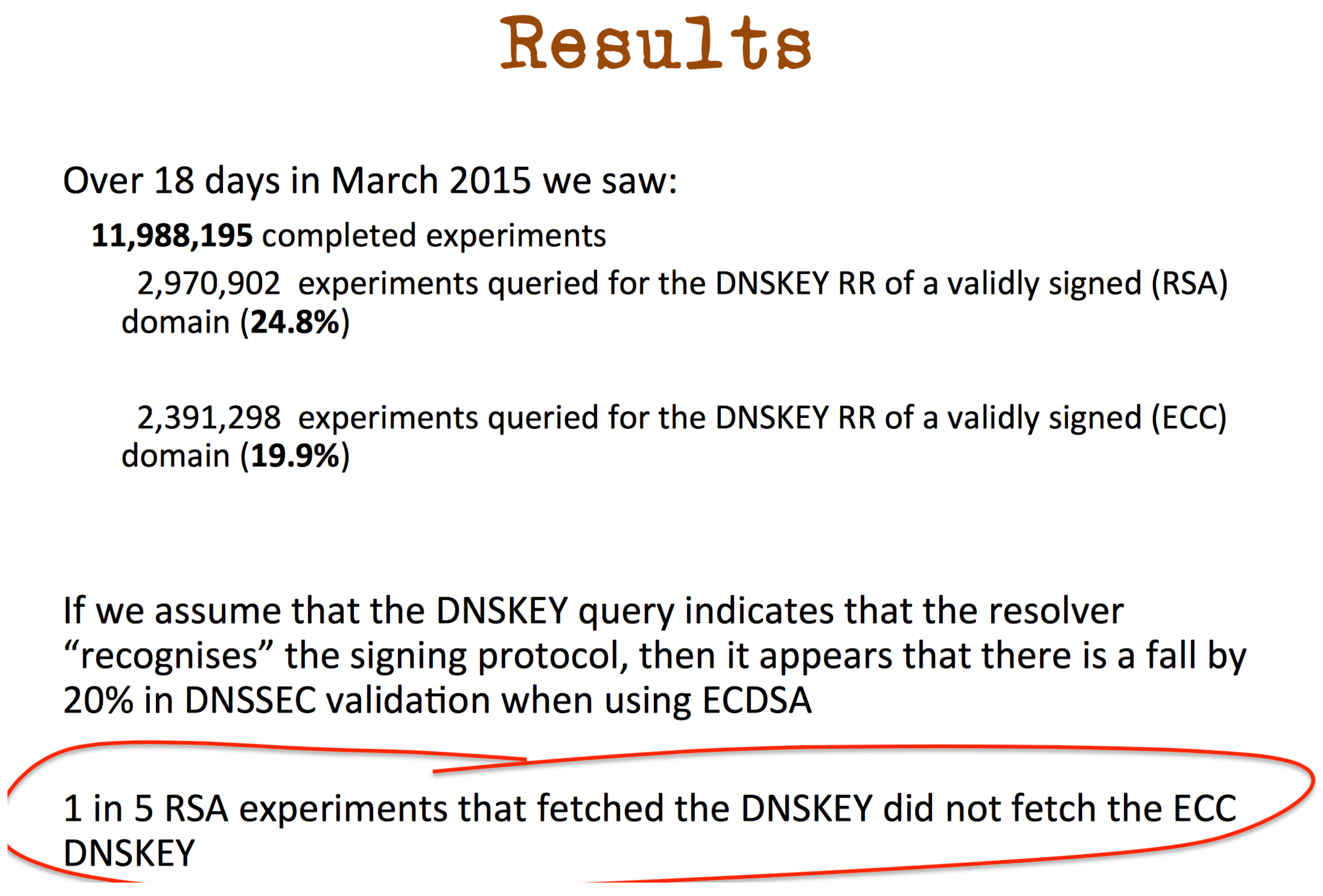
CLOUDFLARE®

ECDSA is your friend

Ólafur Guðmundsson

Why

- ECC is a newer stronger public key
- DNSSEC rfc6605 april 2012
- Smaller keys and signatures
- Signing is fast
- CloudFlare is deploying in 1M+ domains this year



Results

Over 18 days in March 2015 we saw:

11,988,195 completed experiments

2,970,902 experiments queried for the DNSKEY RR of a validly signed (RSA) domain (**24.8%**)

2,391,298 experiments queried for the DNSKEY RR of a validly signed (ECC) domain (**19.9%**)

If we assume that the DNSKEY query indicates that the resolver "recognises" the signing protocol, then it appears that there is a fall by 20% in DNSSEC validation when using ECDSA

1 in 5 RSA experiments that fetched the DNSKEY did not fetch the ECC DNSKEY

Credit: GeoffH

ECC is getting much faster

MacBook Pro 2.2 GHz Intel Core i7 single core performance OpenSSL

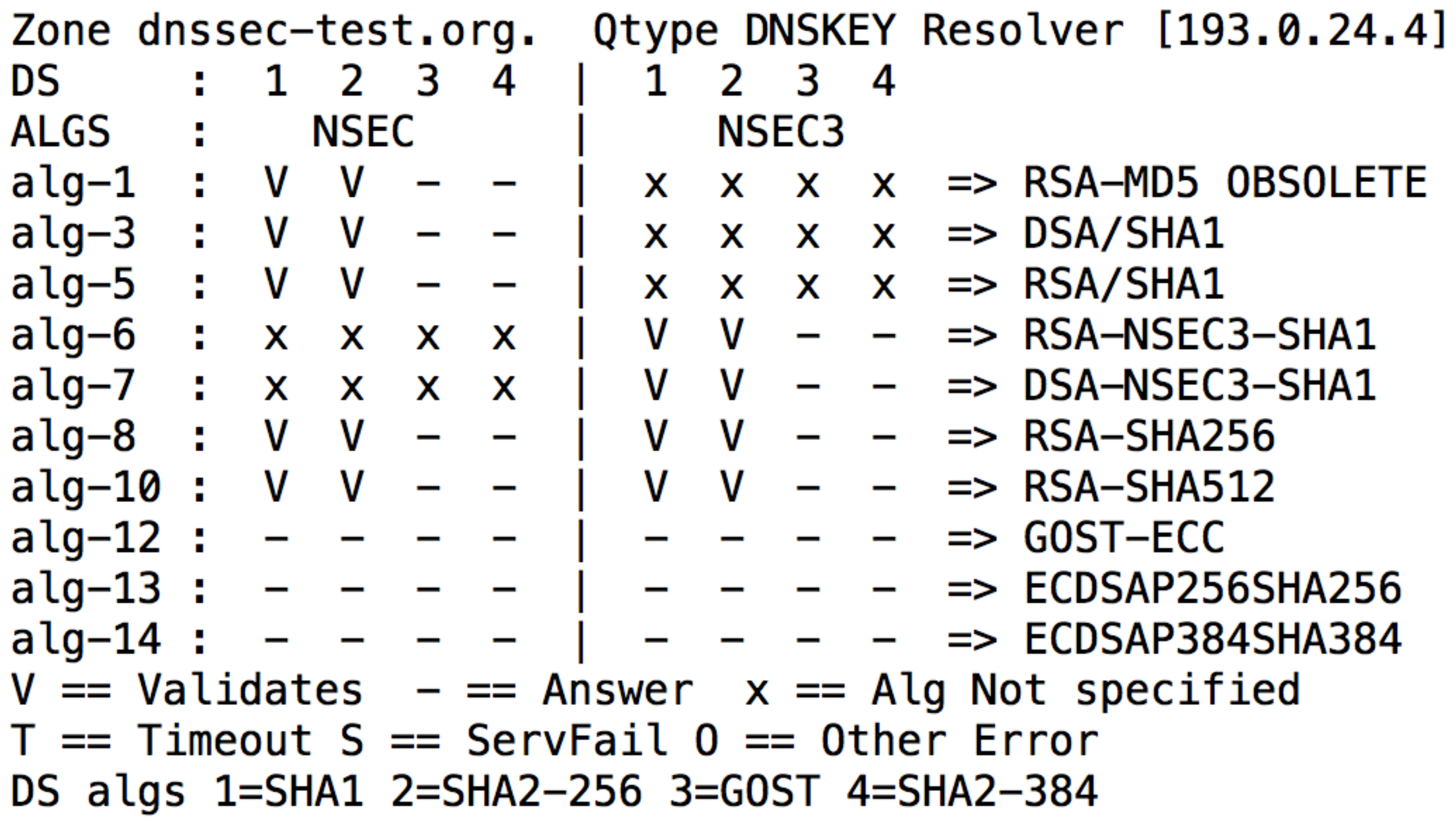
	0.9.8	1.0.2a	
1024 Sign	2,000	6,850	3.5x
2048 Sign	380	1,480	4.5x
ECDSA	5,000	22,000	4.5x
1024 ver	42,300	97,500	2x
2048 ver	15,100	33,000	2x
ECDSA	1,150	9,000	8x

CloudFlare DNSSEC

- Public beta in progress
  - More can join soon
- Product later this year
  - Will sign all/most domains
- Whats included
  - ECDSAP256
  - TLSA records for https, as well CDS or CDNSKEY depending on TLD
  - NSEC zone walking protection

Deployment Stumbling blocks

- Auth servers do not load
- Registries do not allow DS via EPP
- Registrars do not accept DS in UI/API
- Validators do not support
  - https://github.com/ogud/DNSSEC_ALG_Check
- Please HELP FIX



```
Zone dnssec-test.org.  Qtype DNSKEY Resolver [193.0.24.4]
DS      :  1  2  3  4  |  1  2  3  4
ALGS    :    NSEC      |    NSEC3
alg-1   :  V  V  -  -  |  x  x  x  x  => RSA-MD5 OBSOLETE
alg-3   :  V  V  -  -  |  x  x  x  x  => DSA/SHA1
alg-5   :  V  V  -  -  |  x  x  x  x  => RSA/SHA1
alg-6   :  x  x  x  x  |  V  V  -  -  => RSA-NSEC3-SHA1
alg-7   :  x  x  x  x  |  V  V  -  -  => DSA-NSEC3-SHA1
alg-8   :  V  V  -  -  |  V  V  -  -  => RSA-SHA256
alg-10  :  V  V  -  -  |  V  V  -  -  => RSA-SHA512
alg-12  :  -  -  -  -  |  -  -  -  -  => GOST-ECC
alg-13  :  -  -  -  -  |  -  -  -  -  => ECDSAP256SHA256
alg-14  :  -  -  -  -  |  -  -  -  -  => ECDSAP384SHA384
V == Validates   - == Answer   x == Alg Not specified
T == Timeout S == ServFail O == Other Error
DS algs 1=SHA1 2=SHA2-256 3=GOST 4=SHA2-384
```