# Measurement of DNSSEC Validation with Edwards Curve Cryptography

Geoff Huston, Joao Damas APNIC Labs September 2020

## Edwards Curve Cryptography

- Relatively recent crypto offering, first published in 2011
- One of the Elliptic-Curve family of algorithms, using a "twisted Edwards Curve"
- Intended to distinguish itself from other crypto algorithms by being:
  - Faster
  - Unencumbered by lingering IPR disputes
  - High crypto "density"
  - Public domain source code

### I'm really not a crypto geek

- So I'll do a REALLY BRIEF summary of Edwards Curves
- The *normal form* of elliptic curves that Harold Edwards studied in 2007 was:

$$x^2 + y^2 = c^2 + c^2 x^2 y^2$$

- The *twisted transform* of such curves results from the relationship  $ax^2 + y^2 = 1 + dx^2y^2$
- These curves can be used to derive a digital signature algorithm for use in public key cryptography, described in RFC 8032.

### I'm still not a crypto geek

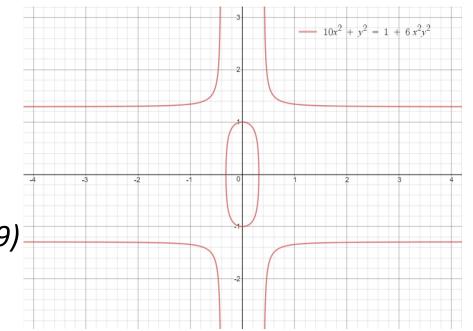
Ed25519 uses an instance of this Edwards Curve curve where:

*a* = -1 and *d* = -121665/121666

and is mapped into a prime field *p* where  $p = 2^{255} - 19$ .

This produces the relationship:

 $-x^{2} + y^{2} = 1 - (121665/121666) x^{2}y^{2} \pmod{2^{255} - 19}$ 



### Ed25519 crypto protocol

Domain Name System Security (DNSSEC) Algorithm Number:		1.1	Reserveu				[Krco/25][proposed standard]		
		12	GOST R 34.10-2001	ECC-GOST	Y	*	[RFC5933][proposed standard]		
		13	ECDSA Curve P-256	ECDSAP256SHA256	Y	*	[RFC6605][proposed standard]		
DNS Security Algorithm Numbers DNS SKY Incode Differentiman Prime Lengths DNS SKY Incode Differentiman Weilschown Prime/Generator Pairs DNS Reco Differentiman Weilschown Prime/Generator Pairs					with SHA-256				
DNS Security Algorithm Numbers				14	ECDSA Curve P-384	ECDSAP384SHA384	Y	*	[RFC6605][proposed standard]
RFC Required Reference [RFC4034][RFC3755][RFC6 Note					with SHA-384				
Where WET, SIG, DENERT, ASIG, SA, and CHET HBE use an 1-bit number used to identify the security algorithm being used. All eloperithm numbers in this registry may be used in CHET HBE. Each signing (OREGO and transaction security secharisms (SIGI)) and BTGO make use of particular subsets of these algorithms. Only algorithms only these useds for SIGIO, and TIGE may repeat it in SIG and HTT MHE. There has been no determined and TIGE may repeat it in SIG and HTT MHE.		15	Ed25519	ED25519	Y	*	[RFC8080][proposed standard]		
		16	EU448	ED448	Y	*	[RFC8080][proposed standard]		
Available Formats									
Number Description	Mnemonic 🖭	Zone Tra Signing Sec							
	DELETE	N N			ď				
0 Delete DS 1 RSA/MD5 (deprecated, see 5)	RSAMD5	N	Y [RFC3110][proposed standard][RFC4034][proposed stand						
	RSAMD5	N Y Y Y	Y [ <u>RFC2539][proposed standard]</u> Y [ <u>RFC3755][proposed standard][RFC2536][proposed stand</u>		sing Standards Publication (FIPS PUB) 186, Digital Signature Standard, ure Hash Standard, 17 April 1995, (Supersedes FIPS PUB 180 dated 11				
1 RSA/MD5 (deprecated, see 5) 2 Diffie-Hellman 3 DSA/SHA1 4 Reserved	RSAMDS 5) DH DSA	N Y Y Y	Y ( <u>RFC2539</u> )[proposed standard] ( <u>RFC2539</u> ][proposed standard] ( <u>RFC2559</u> ][proposed standard][ <u>RFC2539</u> ][proposed stand 18 May 1993.][Federal Information Processing Standards May 1993.]] ( <u>RFC67229</u> ][proposed standard]	Publication (FIPS PUB) 180-1, Secu					
1 RSA/MD5 (deprecated, see 5) 2 Diffie-Hellman 3 DSA/SHA1 4 Reserved 5 RSA/SHA-1	RSAMD5 5) DH DSA RSASHA1	N Y Y Y	Y [ <u>BFC2539]</u> [proposed standard] Y [ <u>BFC2539]</u> [proposed standard][ <u>BFC2539</u> [proposed stand 18 May 1993.]] ( <u>BFC210]</u> [proposed standard] Y [ <u>BFC210]</u> [proposed standard]	Publication (FIPS PUB) 180-1, Secu					
1     RSA/MD5 (deprecated, see 5; (deprecated, see 5; DSA/SHA1       2     Diffie-Hellman       3     DSA/SHA1       4     Reserved       5     RSA/SHA1       6     DSA-NSEC3-SHA1       7     RSASHA1-MSEC3-SHA1	RSAMD5 5) DH DSA RSASHA1 DSA-NSEC3-SHA1 RSASHA1-NSEC3-	Y Y Y Y	Y [ <u>BFC2539]</u> [proposed standard] Y [ <u>BFC2539]</u> [proposed standard][ <u>BFC2539</u> [proposed stand 18 May 1993.]] ( <u>BFC210]</u> [proposed standard] Y [ <u>BFC210]</u> [proposed standard]	Publication (FIPS PUB) 180-1, Secu					
1     RSA/MD5       (deprecated, see 5;     (deprecated, see 5;       2     Diffiel-Hellman       3     DSA/SHA1       4     Reserved       5     RSA/SHA-1       6     DSA-NSEC3-SHA1       7     RSA/SHA-1       7     RSA/SHA-1	RSAMDS 5) DH DSA RSASHA1 DSA-NSEC3-SHA1 RSASHA1-NSEC3- SHA1	N Y Y Y Y Y Y Y	[BECS330](proposed standard] [BECS330](proposed standard] [BECS320](proposed standard) [BECS320](proposed standard) [BECS320](proposed standard) [BECS3110](proposed standard) [BECS3120](proposed standard) [BECS3	Publication (FIPS PUB) 180-1, Secu					
1     RSA/MD5 (deprecated, see 5; (deprecated, see 5; DSA/SHA1       2     Diffie-Hellman       3     DSA/SHA1       4     Reserved       5     RSA/SHA1       6     DSA-NSEC3-SHA1       7     RSASHA1-MSEC3-SHA1	RSAMD5 5) DH DSA RSASHA1 DSA-NSEC3-SHA1 RSASHA1-NSEC3-	Y Y Y Y	(BEC2532)[croposed standard] (BEC2532)[croposed standard] (BEC2532)[croposed standard] (BEC2532)[croposed standard] (BEC2512)[croposed standard] (BEC2512)[croposed standard] (BEC2512)[croposed standard] (BEC2512)[croposed standard]	Publication (FIPS PUB) 180-1, Secu					
1     RSA/M05       2     D://File-Hellman       3     DSX/SHA1       4     Reserved       5     RSX/SHA-1       6     DSA/SHS-15-8H1       7     RSA/SHA-1       8     RSX/SHA-25- SHA1       8     RSX/SHA-25- SHA1	RSAMDS 5) DH DSA RSASHA1 DSA-NSEC3-SHA1 RSASHA1-NSEC3- SHA1	N Y Y Y Y Y Y Y	(BEC2530)[proposed standard] (BEC2530)[proposed standard] (BEC2530)[proposed standard] (BEC252)[proposed standard] (BEC252)[proposed standard] (BEC25110][proposed standard] (BEC25150][proposed standard] (BEC25150][proposed standard] (BEC25150][proposed standard] (BEC25150][proposed standard]	Publication (FIPS PUB) 180-1, Secu					
1     RSAMDS       (depresated, see S     Diffie Hellman       3     DSA/SHA1       4     Reserved       5     RSA/SHA1       6     DSA/SHA1       7     RSA/SHA1       8     RSA/SHA1       9     Reserved       10     RSA/SHA256       11     Reserved       11     Reserved	RSAMDS DH DSA RSASHA1 DSA-NSEC3-SHA1 RSASHA1-NSEC3- SHA1 RSASHA256 RSASHA256 RSASHA212	N ) Y ) Y ) Y ) Y ) Y ) Y )	(BEC2530)[proposed standard] (BEC2530)[proposed standard] (BEC2530)[proposed standard] (BEC252)[proposed standard] (BEC252)[proposed standard] (BEC25110][proposed standard] (BEC25150][proposed standard]	Publication (FIPS PUB) 180-1, Secu					
1     RSAMDS       (depretated see 5)     Quifie-Heliman       3     DSA/SHA1       4     Reserved       5     RSA/SHA1       6     DSA/SHA1       7     RSA/SHA1       8     RSA/SHA1-NSEC3-SHA1       8     RSA/SHA1-NSEC3-SHA1       8     RSA/SHA2-S6       9     Reserved       10     RSA/SHA1-S12	RSAMDS DH DSA RSASHA1 DSA-NSEC3-SHA1 RSASHA1-NSEC3- SHA1 RSASHA256 RSASHA512 D1 ECC-GOST	N ) Y ) Y ) Y ) Y ) Y ) Y )	(BEC2530)[proposed standard] (BEC2530)[proposed standard] (BEC2530)[proposed standard] (BEC252)[proposed standard] (BEC2510)[proposed standard]	Publication (FIPS PUB) 180-1, Secu					
1     RSAVBC       (depractal see S)     Diffie Hellman       3     DSA/SHA1       4     Reserved       5     RSAVELA1       6     DSA/SHA1       7     RSAVELA1       8     RSAVSHA1       9     Reserved       10     RSAVSHA256       9     Reserved       10     RSAVSHA5126       11     Reserved       12     GOST R 34.1-SOCCAUPP 2/35       13     ECOSA Curve P2/35	S     RSAMDS       S)     DH       DSA     DSA       RSASHA1     DSA/NSEC3-SHA1       DSA/NSEC3-SHA1     RSASHA256       RSASHA1:NSEC3-SHA1     RSASHA256       RSASHA256     RSASHA256       CCGOST     ECC-GOST       ECDSAP2565THA256     ECDSAP2565THA256	N Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y	(BEC2332)[proposed standard] (BEC2332)[proposed standard] (BEC2332)[proposed standard] (BEC2332)[proposed standard] (BEC2312)[proposed standard] (BEC23110][proposed standard] (BEC23110][proposed standard] (BEC2312)[proposed standar	Publication (FIPS PUB) 180-1, Secu					
1     RSAMDS       (depreated, see S     Diffie-Hellman       3     DSA/SHA1       4     Reserved       5     RSA/SHA1       6     DSA/SHA1       7     RSA/SHA1       7     RSA/SHA1-NSEC3-SHA1       8     RSA/SHA1-NSEC3-SHA1       9     Reserved       10     RSA/SHA256       9     Reserved       11     Reserved       12     GOST R 34.1-20G       13     ECDSA-Curve P.34       14     ECDSA-Curve P.34       15     EdJSS19	RSAMDS       DH       DSA       RSASHA1       DSA       RSASHA1       DSA       RSASHA1       DSA       RSASHA1       RSASHA256       RSASHA256       RSASHA256       RSASHA256       RSASHA512       COSST6       ECDSAP384SHA384       ED25519	N Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y	(BEC2530)[proposed standard] (BEC2530)[proposed standard] (BEC2530)[proposed standard] (BEC2510)[proposed standard] (BEC25110][proposed standard] (BEC25150][proposed standard] (BEC25150[[proposed standard]]	Publication (FIPS PUB) 180-1, Secu					
1     RSXMDS       (depreated, see 5)     Diffie-Hellman       3     DSX/SHA1       4     Reserved       5     RSX/SHA1       6     DSX/SHA1       7     RSS/SHA1       7     RSS/SHA1       8     RSX/SHA1       9     Reserved       9     Reserved       10     RSX/SHA512       11     Reserved       12     GOST R A1-02001       12     GOST R A1-02001       13     ECDSA Curve P 28       14     ECDSA Curve P 28       15     Ed25519       16     Ed448	8:SAMDS       DH       DS       RSASHAT       DS-N-NSEC3-SHAT       DS-N-NSEC3-SHAT       RSASHAT2       RSASHAT2       RSASHAT26       RSASHAT26       RSASHAT264       CCG-05T       ECC-005T       ECCSAP2665HA256       RCAP3845HA384	N Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y	()     (BEC233)[[proposed standard]     (BEC233)[[proposed standard]     (BEC233)[[proposed standard]     (BEC233)[[proposed standard]     (BEC233)[[proposed standard]     (BEC231)[[proposed standard]     (BEC232)[[proposed standa	Publication (FIPS PUB) 180-1, Secu					
1     RSA/MDS       (deprecated, see S2     Diffie-Hellman       3     DSA/SHA1       4     Reserved       5     RSA/SHA1       6     DSA/SHA1       7     RSSA/SHA1       7     RSSA/SHA1-SEC3-SHA1       8     RSA/SHA-SEC3       9     Reserved       10     RSA/SHA-SE23       9     Reserved       11     Reference       12     GOST R 34-10-2001       13     ECDSA-Curve P38-with 54-354       14     ECDSA-Curve P38-with 54-384       15     Ed25519       16     Ed484       17-122     Unassigned	RSAMDS       DH       DSA       RSASHA1       DSA       RSASHA1       DSA       RSASHA1       DSA       RSASHA1       RSASHA256       RSASHA256       RSASHA256       RSASHA256       RSASHA512       COSST6       ECDSAP384SHA384       ED25519	N Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y	(BEC2530)[proposed standard] (BEC2530)[proposed standard] (BEC2530)[proposed standard] (BEC2530][proposed standard] (BEC2510][proposed standard] (BEC2515][proposed standard]	Publication (PPS PUB) 180-1, Sec					
1     RSA/MDS       (depreated, see 5)     Diffie-Hellman       3     DSA/SHA1       4     Reserved       5     RSA/SHA1       6     DSA/SHA1       7     RSSA/SHA1       7     RSSA/SHA1       8     RSA/SHA1-ABEC3-SHA1       9     Reserved       10     RSA/SHA1-ASEC3-SHA1       2     GOST RSA1-SA2C3       10     RSA/SHA1-S2C6       9     Reserved       10     RSA/SHA1-S2C6       9     RESERVED       10     RSA/SHA1-S2C6       9     RESERVED       10     RSA/SHA1-S2C6       9     RESERVED       10     RSA/SHA1-S2C6       11     Reserved       12     GOST RA 1-0-2001       13     ECDSA Curve P-38       14     ECDSA Curve P-38       15     Ed42519       16     Ed448	8:8AMD5       0)       0H       0SA       RSASHA1       DSA-NSEC3-SHA1       RSASHA1       DSA-NSEC3-SHA1       RSASHA1       RSASHA1       DSA-NSEC3-SHA1       RSASHA1       RSASHA12       D1     ECC-GOST       ECDSAP2865HA256       ED25519       ED48	N Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y	()     [BEC2330](proposed standard)     [BEC2330](proposed standard)     [BEC2330](proposed standard)     [BEC2330](proposed standard)     [BEC2330](proposed standard)     [BEC23110](proposed standard)     [BEC23110](proposed standard)     [BEC23120](proposed standard)     [BEC2320](proposed standard)     [BEC2320](propo	Publication (PPS PUB) 180-1, Sec					
1     RSA/MDS       (depreated, see 5)     Diffie-Hellman       3     DSA/SHA1       4     Reserved       5     RSA/SHA1       6     DSA/SHA1       7     RSSA/SHA1       8     RSA/SHA1       9     Reserved       9     Reserved       10     RSA/SHA1-SEC3-SHA1       21     OSTA/SHA1-SEC3-SHA1       22     RSA/SHA1-SEC3-SHA1       20     RSTA/SHA512       10     RSA/SHA1-SEC3-SHA1       2     GOT R A1-0-2001       2     GOT R A1-0-2001       12     GOT R A1-0-2001       13     ECDSA Curve P 234       14     ECDSA Curve P 244       15     Ed2S519       16     Ed448       17-122     Unassigned       172-22     Reserved for Indira       172-23     Reserved for Standary       172-24     Reserved for Indira	8.8AMDS       01       04       05A       RSASHAT       05A       RSASHAT       05A       RSASHAT       05A       RSASHAT       05A-NSEC3-SHAT       RSASHATS2       SHAT       RSASHATS2       01     ECC-GOST       6     ECDSAP2865HA256       ED2519     ED48       ED48     NDIRECT	X X X X X X X X X X X X X X X X X X X	IBEC2330[[croposed standard]     IBEC2330[[croposed standard] <td< td=""><td>Publication (PPS PUB) 180-1, Sec</td><td></td><td></td><td></td><td></td><td></td></td<>	Publication (PPS PUB) 180-1, Sec					
1     RSA/MDS       (deprecated, see 5;     Diffie-Hellman       3     DSA/SHA1       4     Reserved       5     RSA/SHA1       6     DSA/SHA1       7     RSSA/SHA1       7     RSSA/SHA1       8     RSA/SHA1-SEC3       9     Reserved       10     RSA/SHA-S12       11     Reserved       12     GDST R 34.10-2001       13     ECDSA Curve P34       with SHA-S12     RSSF14       14     ECDSA Curve P34       15     Ed5519       16     Ed48       17-122     Unassigned       123-252     Reserved for Indiri	RSARMDS       DH       DSA       RSASHA1       DSA       RSASHA1       DSA       RSASHA1       DSA       RSASHA1       RSASHA1       RSASHA1       RSASHA1       RSASHA256       RSASHA256       RSASHA258       COST       ED25519       ED48       ED25519       ED48       INDIRECT       PRIVATEDNS	V V V V V V V V V V V V V V V V V V V	()     [BEC2330](proposed standard)     [BEC2330](proposed standard)     [BEC2330](proposed standard)     [BEC2330](proposed standard)     [BEC2330](proposed standard)     [BEC23110](proposed standard)     [BEC23110](proposed standard)     [BEC23110](proposed standard)     [BEC23120](proposed standard)     [BEC23120](proposed standard)     [BEC23120](proposed standard)     [BEC23120](proposed standard)     [BEC23120](proposed standard)     [BEC232020](proposed standard)     [BEC233200](proposed standard)     [BEC2	Publication (PPS PUB) 180-1, Sec					

https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml

#### Ed25519 Evaluation

#### 1. Key Size

Algorithm	Private Key	Public Key	Signature Record
Ed25519	179 bytes	300 bytes	146 bytes
ECDSA P-256	187 bytes	353 bytes	146 bytes
RSA-2048	1,776 bytes	620 bytes	403 bytes
RSA-4096	3,312 bytes	967 bytes	744 bytes

#### Ed25519 Evaluation

2. Key Processing Time

zone with 500K entries, OpenSSL 1.1.1k libraries on a FreeBSD 12.2 host with the DNSSEC toolset supplied with Bind 9.16.16. Validation time is elapsed time for 50K queries with DNSSEC validation

Algorithm	Signing Time	Relative	Validation Time
Unsigned			905 secs
Ed25519	800 secs	1	1,008 secs
ECDSA P-256	450 secs	0.56	1,036 secs
RSA-2048	3,000 secs	3.75	1,173 secs
RSA-4096	3,312 secs	4.14	1,176 secs

### Validation Support for Ed25519

We used an ad-based measurement to measure the support for Ed25519

- Control URL unsigned DNS name
- Positive URL signed with Ed25519
- Negative URL bad Ed25519 RRSIG record

What happens when a resolver does not support a signing protocol? It treats the name as **unsigned** (RFC 4035)

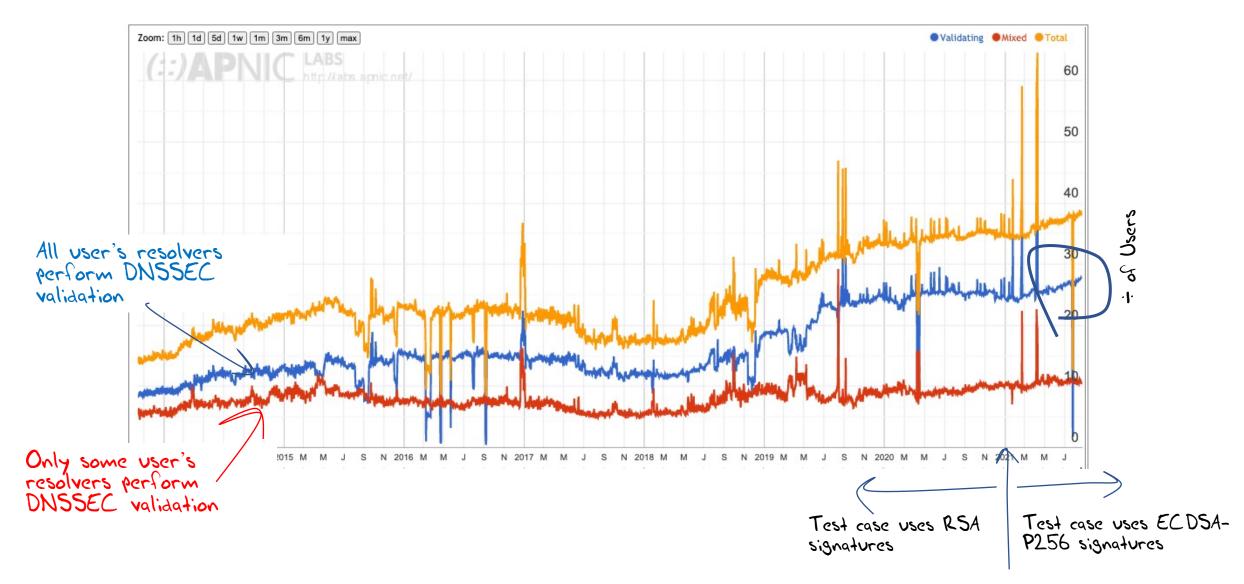
### A user is recorded as **supporting** Ed25519

- We observe A/AAAA queries for both DNS names
- We observe DNSKEY and DS queries for both DNS names
- We observe a web fetch for the valid URI and no web fetch for the invalid URI
- The inference of the invalid condition is that <u>all</u> the recursive resolvers need to support ED25519 for the test to record a positive result

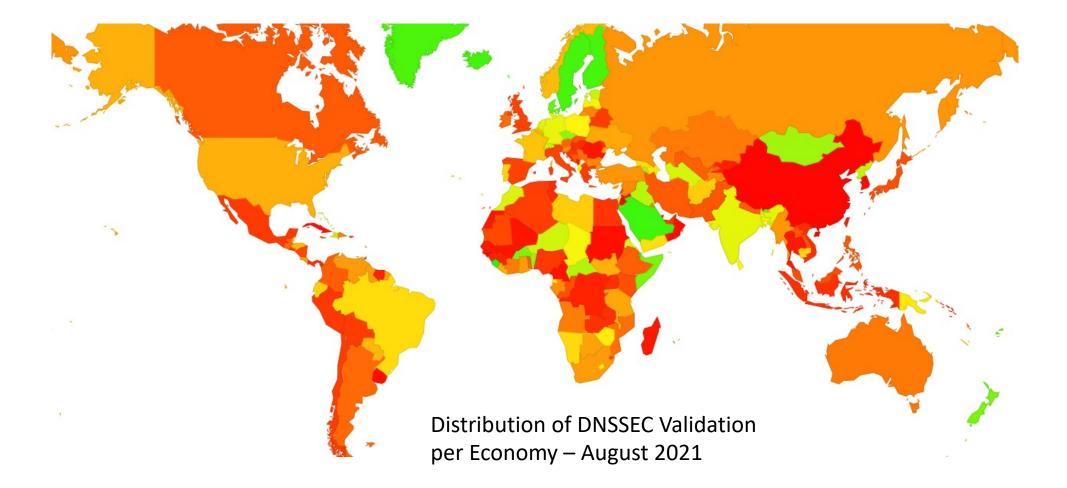
### A user is recorded as **NOT supporting** Ed25519

- We observe A/AAAA queries for both DNS names
- If we observe DNSKEY and DS queries for both DNS names then we call this "mixed" support
- We observe a web fetch for the valid URI and a web fetch for the invalid URI

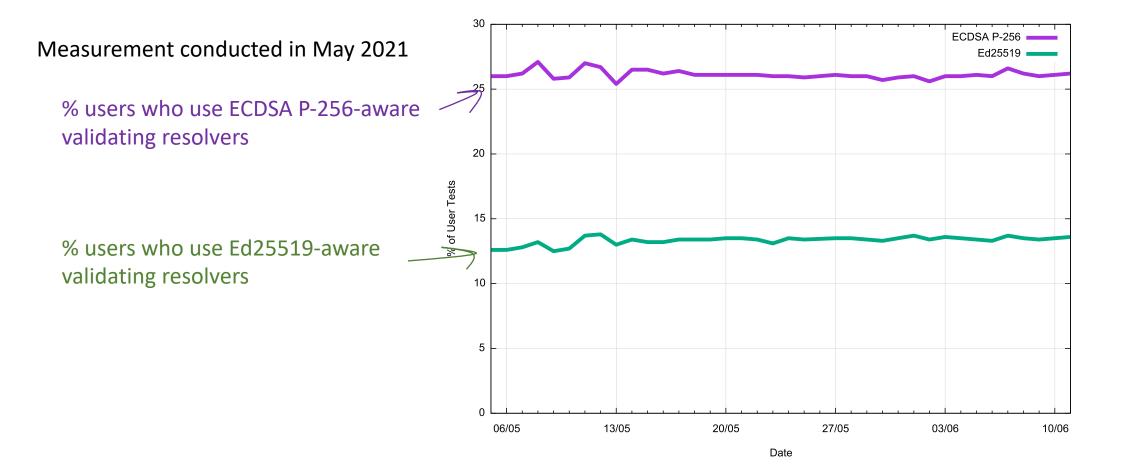
### What is a DNSSEC validation "baseline"?



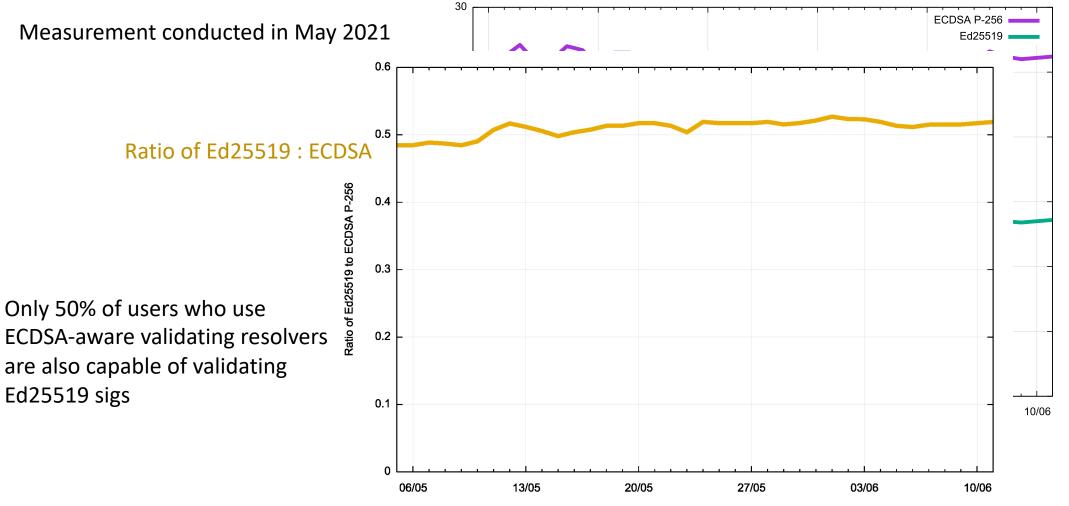
#### What is a DNSSEC validation "baseline"?



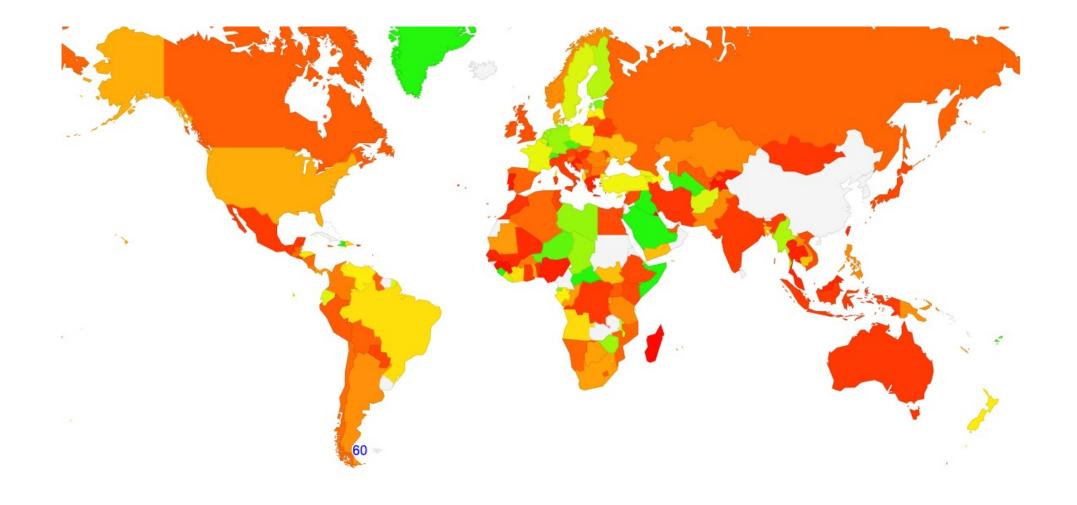
#### ECDSA P-256 vs Ed25519



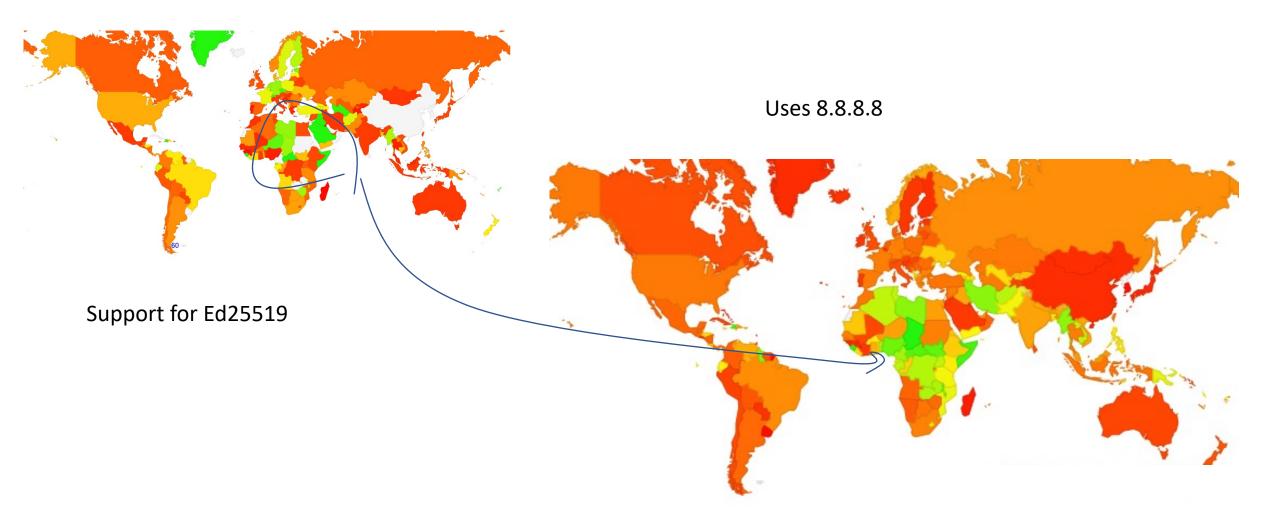
#### ECDSA P-256 vs Ed25519



### Where?



#### Is this due to Google's 8.8.8.8 Service?



There is a reasonable correlation in Africa, but less so elsewhere

#### **ISP** View

List of the "largest" ISPs whose resolvers support ECDSA, but do not support Ed25519 for DNSSEC validation

AS	СС	Count	ECDSA	Ratio	Ed25519	Ratio	AS Name
55836	IN	22998060	21848577	0.95	899647	0.04	Reliance Jio, India
7922	US	4070748	3975062	0.98	251901	0.06	COMCAST, USA
36903	MA	2070044	1677701	0.81	148415	0.07	MT-MPLS, Morocco
36992	EG	885949	393591	0.44	64321	0.07	ETISALAT-MISR, Egypt
45245	BD	851055	670971	0.79	22466	0.03	BANGLALINK, Bangladesh
4818	MY	657060	610952	0.93	9234	0.01	DIGIIX, Malaysia
3243	PT	614634	605322	0.98	11220	0.02	MEO-RESIDENCIAL, Portugal
30689	JM	604787	370476	0.61	48738	0.08	FLOW-NET, Jamacia
45727	ID	599026	281679	0.47	27017	0.05	Hutchison, Indonesia
35819	SA	524105	471071	0.90	13819	0.03	Etihad Etisalat, Saudi Arabia
25144	BA	416270	174427	0.42	38926	0.09	TELEKOM-SRPSKE, Bosnia
43766	SA	330041	309512	0.94	10440	0.03	MTC-KSA, Saudi Arabia
8359	RU	281142	273762	0.97	4561	0.02	MTS, Russia
23889	MU	272176	267050	0.98	7127	0.03	Mauritius Telecom, Mauritius
17882	MN	255505	203365	0.80	24229	0.09	MCS, Mongolia
1241	GR	225024	221091	0.98	6626	0.03	Forthnet, Greece
26615	BR	194565	92371	0.47	18433	0.09	TIM, Brazil
37133	ΤZ	185453	182966	0.99	1529	0.01	AIRTEL, Tanzania
47589	KW	179303	152935	0.85	1207	0.01	KTC, Kuwait
4804	AU	154869	123355	0.80	2380	0.02	Microplex, Australia
6871	GB	133194	112411	0.84	3941	0.03	PLUSNET, UK
9231	ΗК	114751	89091	0.78	846	0.01	China Mobile Hong Kong, Hong
39603	PL	114310	112859	0.99	1380	0.01	P4NET, Poland
15146	BS	111989	108602	0.97	2871	0.03	CABLEBAHAMAS, Bahamas
37424	BJ	110672	107193	0.97	933	0.01	Spacetel, Benin
12083	US	110585	106278	0.96	10258	0.09	WOW-INTERNET, USA
34058	UA	109748	108367	0.99	1530	0.01	LIFECELL, Ukraine
44143	RS	102026	100691	0.99	1178	0.01	A1SERBIA, Serbia
16086	FI	99675	98390	0.99	1233	0.01	DNA, Finland
29244	BG	97964	96725	0.99	286	0.00	TELENORBG, Bulgaria

### Is Ed25519 viable for DNSSEC?

No, not today

It has smaller keys and signatures than RSA-2048

It is the same size as ECDSA

It is a lot faster to sign a zone than RSA-2048 but a lot slower than ECDSA (2x)

It is (a little) faster to validate than ECDSA and RSA

But...

It is really not adequately supported by DNSSEC-validating resolvers deployed today

#### Questions?