NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

Trustworthy Networking Program

RIB Size Estimation for BGPSEC

K. Sriram

(with O. Borchert, O. Kim, D. Cooper, and D. Montgomery)

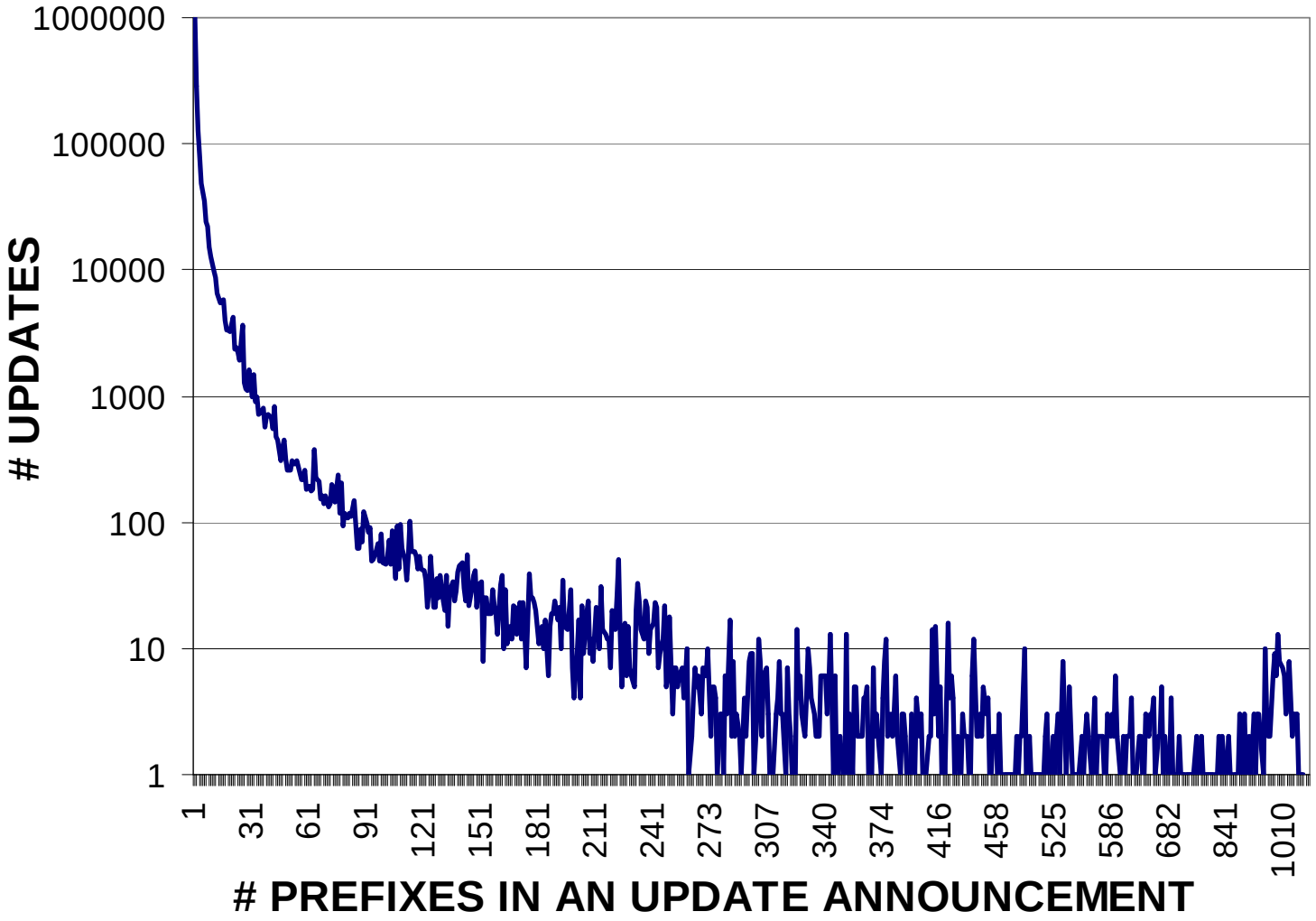
May 24, 2011

Contacts: ksriram@nist.gov, dougm@nist.gov

Acknowledgements: Many thanks are due to the BGPSEC Design Team for comments and suggestions.

This research was supported by the Department of Homeland Security under the Secure Protocols for the Routing Infrastructure (SPRI) program and the NIST Information Technology Laboratory Cyber and Network Security Program.

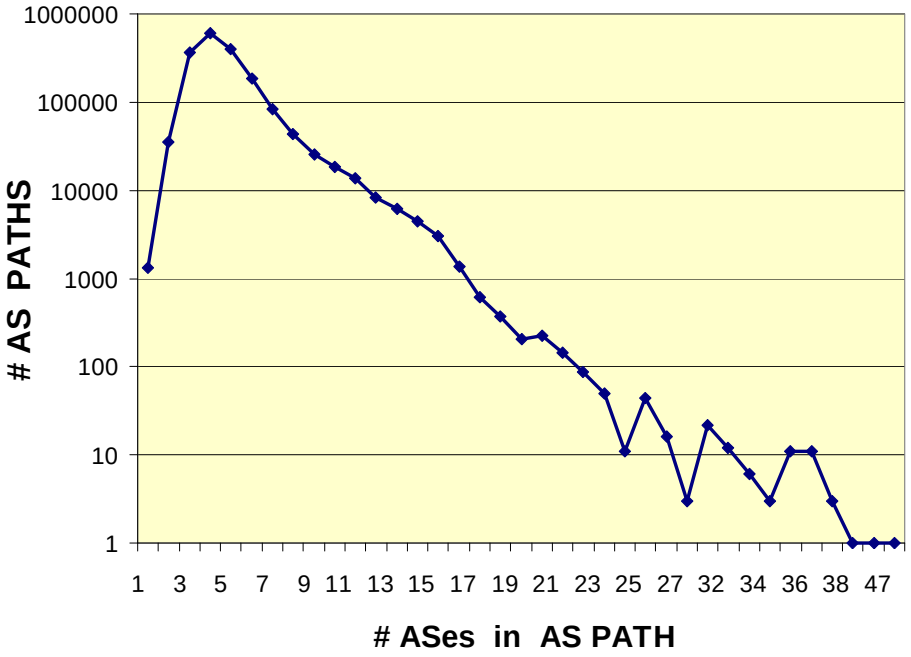
Distribution of # Prefixes in eBGP Announcements



Avg. = 3.832
Std. Dev. = 4.19

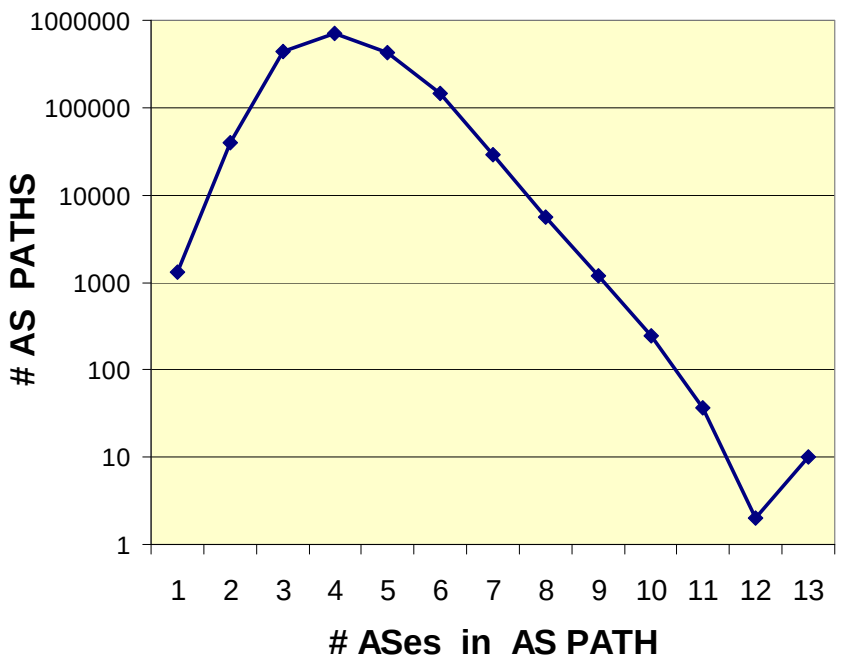
Distribution of AS Path Length in eBGP Announcements

Prepended/Repeat ASes Not Collapsed



- Avg. AS Path Length = 3.743
- Std. Dev. of Path Length = 1.92
- Prob. {AS Path Length $\leq$ 10} = 97.82 %
- Prob. {AS Path Length < 12} = 99.06 %

Prepended/Repeat ASes Collapsed



- Avg. AS Path Length = 3.17
- Std. Dev. of Path Length = 1.05
- Prob. {AS Path Length < 6} = 97.98 %
- Prob. {AS Path Length < 7} = 99.6 %

Measurement of Prefixes and Paths in ISP's Route Reflectors and PE Routers

Measurement data from a Large, Tier 1 ISP

	Provider Edge (PE) routers	Route Reflectors (RR)
# Unique Prefixes Observed	377,000	377,000
Total number of Prefix Paths Observed (Low)	750,000	3,100,000
Total number of Prefix Paths Observed (High)	1,100,000	3,600,000
Ratio of Total # Prefix Paths / # Unique Prefixes (High)	2.92	9.55

Update Format and Signature Overheads

Update Element	Octets (RSA-2048 Alg.)
NLRI Length	1
NLRI	4
AS-n	4
AS-(n-1)	4
…	4
AS2	4
AS1 (Originating AS)	4
AS-(n+1) (ASN of Subsequent AS)	4
Expire Time	8
Algorithm Suite Itentifier	1
Signature-List Block Length	2
SKI Length-n	1
SKI-n	20
Signature-n	256
SKI Length-(n-1)	1
SKI-(n-1)	20
Signature-(n-1)	256
…	
…	
…	
SKI Length-2	1
SKI-2	20
Signature-2	256
SKI Length-1	1
SKI-1	20
Signature-1	256
Other BGP Attributes (besides NLRI & AS_PATH; measured/estimated)	40
Estimated Signed Update Size (average)	1188
Measured Unsigned BGP Update Size (average including all BGP attributes)	78

Signature overheads

4 ASes per AS path (see Slide 3)

15x increase in update size (with RSA-2048)

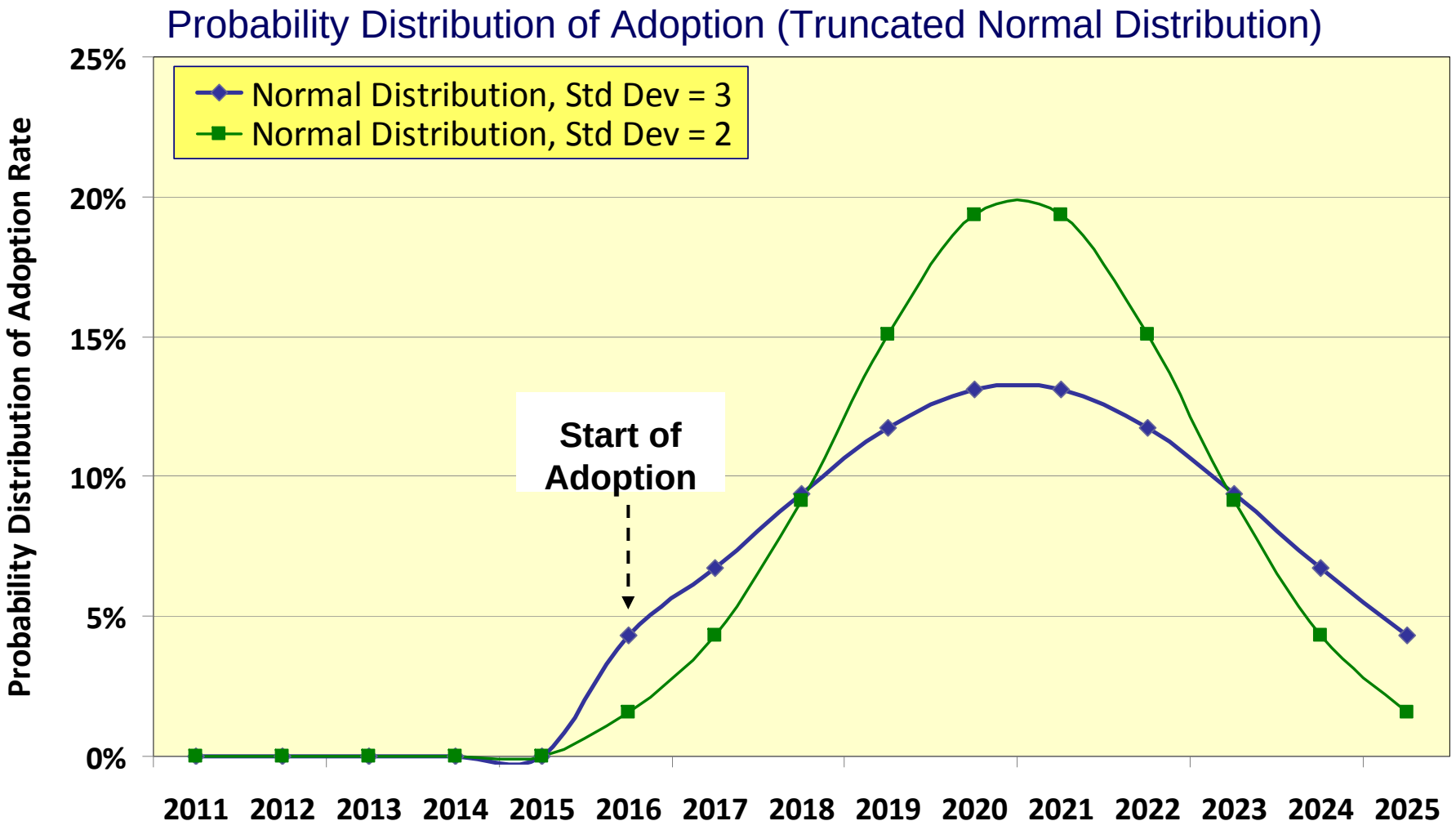
Reference: draft-lepinski-bgpsec-protocol

Estimation of BGPSEC Update Sizes

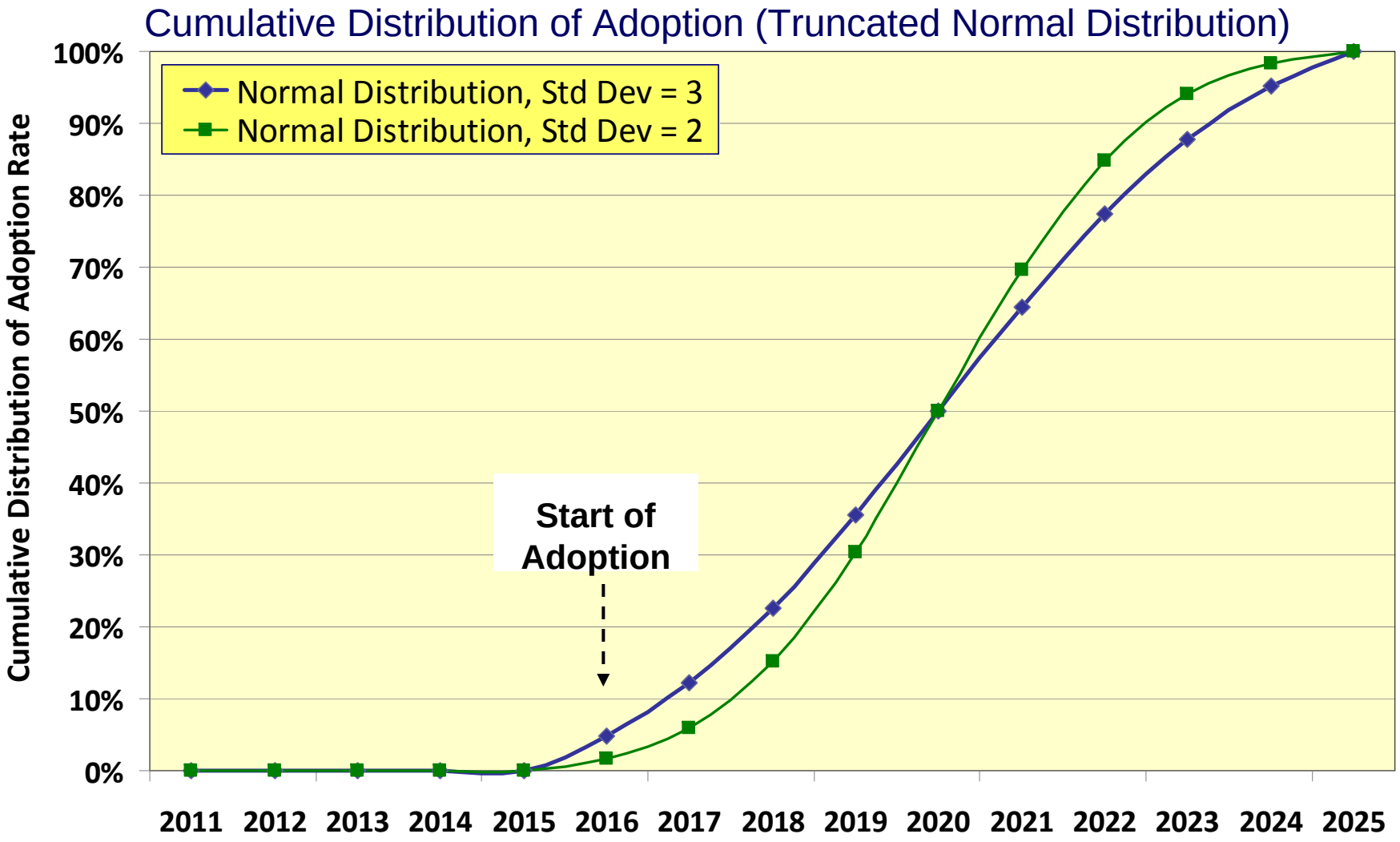
	eBGP Update Size (Octets)	Multiplier Relative to Unsigned
Unsigned	78	1.00
RSA-2048	1188	15.23
ECDSA-256	420	5.38
ECDSA-224	388	4.97

- It should also be noted that eBGP updates in BGP-4 average 3.83 prefixes per update (see Slide 2) whereas the same in BGPSEC have only a single prefix per update (un-optimized).
- Unsigned update size was measured from Routeviews data.
- Signed update sizes are estimated (as illustrated in Slide 5).

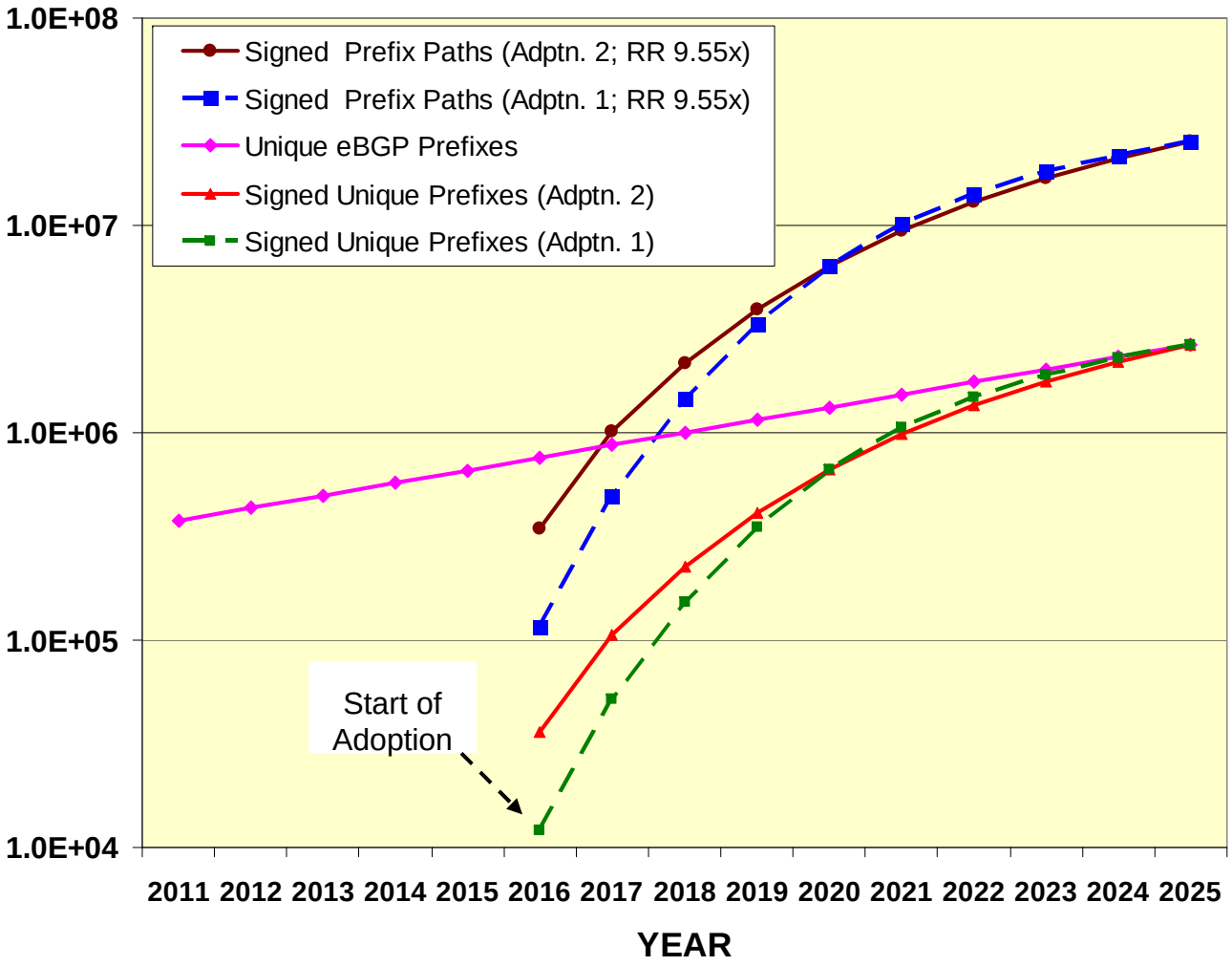
BGPSEC Adoption Rate (1)



BGPSEC Adoption Rate (2)



Projection of eBGP Prefixes and Signed Prefix Paths (1)



- Adptn. 1 means adoption with Normal distribution with Std. Dev. = 2 (see Slides 7, 8)
- Adptn. 2 means adoption with Normal distribution with Std. Dev. = 3 (see Slides 7, 8)
- RR means Route Reflector
- Prefix-path multiplication factor for RR = 9.55

- Growth in eBGP prefixes is assumed to be 15% annually [1].

[1] Geoff Huston, “BGP in 2008,” http://www.potaroo.net/ispcol/2009-03/bgp2008.html

Projection of eBGP Prefixes and Signed Prefix Paths (2)

- In the following data and plots, we will assume Adoption 1 (truncated Normal distribution of adoption with Std. Dev. =2) unless otherwise stated.

Parameters for Estimation of RIB Size

Parameters for Estimation of RIB Size in a BGP Router	Value	Units	Comment
Average update size w/o signatures	78	Octets	Measured (2/09)
Average update size with signatures (RSA-2048 signature alg)	1188	Octets	Estimated
Average update size with signatures (ECDSA-256 signature alg)	420	Octets	Estimated
Average RIB data structure overhead per update (fraction)	5%		Assumption
Avg. number of peers from which update is received for each eBGP prefix at RR	9.55		Measured (RR, Large, Tier 1 ISP)
Avg. number of peers from which update is received for each eBGP prefix at PE	2.92		Measured (PE, Large, Tier 1 ISP)
Avg. number of peers from which update is received for each internal prefix (PE or RR)	10		Assumption
Average # ASes in AS path	3.743		Measured (2/09)
Average # prefixes per update announcement	3.832		Measured (2/09)
Growth rate per year for Internal prefixes	5%		Assumption
Growth rate per year for External prefixes	15%		To extend growth projections further out from Geoff Huston's [1] time window
Include Internal prefixes?	1		1 = YES; 0 = NO

- For BGPSEC, we rounded up the Avg. # ASes in AS path to 4 (from 3.743)
- The model (see next slide) predicts the impact on the RIB size due to signatures

[1] Geoff Huston, “BGP in 2008,” http://www.potaroo.net/ispcol/2009-03/bgp2008.html

Methodology for RIB Size Estimation

Parameters for Estimation of RIB Size in a BGP Router	Symbol	Units	Equation (Model)
Average update size w/o signatures	U	Octets	
Average RIB data structure overhead per update (fraction)	x		
Average memory requirement per update in RIB	Ur	Octets	Ur = U*(1+x)
Avg. number of peers from which update is received for each eBGP prefix	Nu		
Avg. number of peers from which update is received for each internal prefix	m		
Average # prefixes per update announcement	p		
Total # Unique Internal Prefixes with routes in the BGP speaker	Pi		
Total # Unique eBGP Prefixes with routes in the BGP speaker	Pe		
RIB memory consumed by internal prefixes	iRIB	GB	iRIB = (Pi/p)*m*Ur/10^9
Average update size with signatures	Ua	Octets	
Fraction of eBGP updates that are signed (adoption factor)	f		
RIB memory consumed by eBGP updates (BGP-4)	eRIBu	GB	eRIBu = (Pe/p)*Nu*U*(1+x)/10^9
RIB memory consumed by all eBGP updates (fraction f are BGPSEC; fraction (1-f) are unsigned)	eRIBs	GB	eRIBs = [Pe*f*Nu*Ua + {Pe*(1-f)/p}*Nu*U]*(1+x)/10^9
Total RIB memory (BGPSEC)	RIBu	GB	RIBu = iRIB + eRIBu
Total RIB memory (BGP-4)	RIBs	GB	RIBs = iRIB + eRIBs

- The model predicts the impact on RIB size due to signatures in eBGP updates as well as details various components that contribute to RIB size.
- The model includes contribution to RIB size due to internal prefixes (although relatively insignificant).

Unique Prefixes and Prefix Paths

- Estimates for Route Reflector (prefix-path multiplier factor = 9.55 (for eBGP) and 10 (for internal prefixes) ; also see Slide 4)
- Adoption Model 1 (see Slides 7-9)

						BGPSEC (at RR)	
Year	# Unique Internal Prefixes	# Unique External (eBGP) prefixes	Total # Internal Prefix Paths	# Unique eBGP prefixes in BGPSEC Adoption (Signed)	# Unique Unsigned eBGP prefixes	Total # BGPSEC Signed Prefix Paths	Total # Unsigned eBGP Prefix Paths
2011	800000	377000	8000000	0	377000	0	3600000
2012	840000	433550	8400000	0	433550	0	4140000
2013	882000	498583	8820000	0	498583	0	4761000
2014	926100	573370	9261000	0	573370	0	5475150
2015	972405	659375	9724050	0	659375	0	6296423
2016	1021025	758282	10210253	12174	746108	116252	7124634
2017	1072077	872024	10720765	52057	819967	497095	7829923
2018	1125680	1002827	11256803	152516	850311	1456390	8119682
2019	1181964	1153252	11819644	351063	802189	3352322	7660160
2020	1241063	1326239	12410626	663120	663120	6332177	6332177
2021	1303116	1525175	13031157	1060895	464280	10130562	4433446
2022	1368271	1753952	13682715	1487199	266752	14201374	2547235
2023	1436685	2017044	14366851	1896633	120411	18111088	1149812
2024	1508519	2319601	15085193	2282360	37241	21794419	355617
2025	1583945	2667541	15839453	2667541	0	25472541	0

- Growth in eBGP prefixes is assumed to be 15% annually (see Slide 11)
- Growth in internal prefixes is assumed to be 5% annually (see Slide 11)

RIB Size Estimation - Detailed Data

- RSA-2048 and ECDSA-256 signature algorithms
- For the prefix-path projections as shown in Slide 13

	BGP-4 (RR)			BGPSEC (RR, RSA-2048)			BGPSEC (RR, ECDSA-256)		
Year	RIB Requirement for Internal Prefix Paths (GB)	RIB Requirement for External (eBGP) Prefix Paths (GB)	Total RIB size (GB)	Portion of RIB due to Unsigned eBGP Prefix Paths	RIB size for eBGP Prefix Paths with Signatures (GB)	Total RIB size (GB)	Portion of RIB due to Unsigned eBGP Prefix Paths	RIB size for eBGP Prefix Paths with Signatures (GB)	Total RIB size (GB)
2011	0.17	0.08	0.25	0.08	0.01	0.26	0.08	0.00	0.26
2012	0.18	0.09	0.27	0.09	0.01	0.28	0.09	0.00	0.28
2013	0.19	0.10	0.29	0.10	0.01	0.30	0.10	0.00	0.30
2014	0.20	0.12	0.31	0.12	0.01	0.32	0.12	0.00	0.32
2015	0.21	0.13	0.34	0.13	0.01	0.35	0.13	0.00	0.35
2016	0.22	0.15	0.37	0.15	0.15	0.51	0.15	0.05	0.42
2017	0.23	0.18	0.41	0.17	0.62	1.01	0.17	0.22	0.61
2018	0.24	0.20	0.44	0.17	1.82	2.23	0.17	0.64	1.05
2019	0.25	0.23	0.49	0.16	4.18	4.60	0.16	1.48	1.89
2020	0.26	0.27	0.53	0.13	7.90	8.30	0.13	2.79	3.19
2021	0.28	0.31	0.59	0.09	12.64	13.01	0.09	4.47	4.84
2022	0.29	0.36	0.65	0.05	17.71	18.06	0.05	6.26	6.61
2023	0.31	0.41	0.72	0.02	22.59	22.92	0.02	7.99	8.32
2024	0.32	0.47	0.79	0.01	27.19	27.51	0.01	9.61	9.94
2025	0.34	0.54	0.88	0.00	31.77	32.11	0.00	11.23	11.57

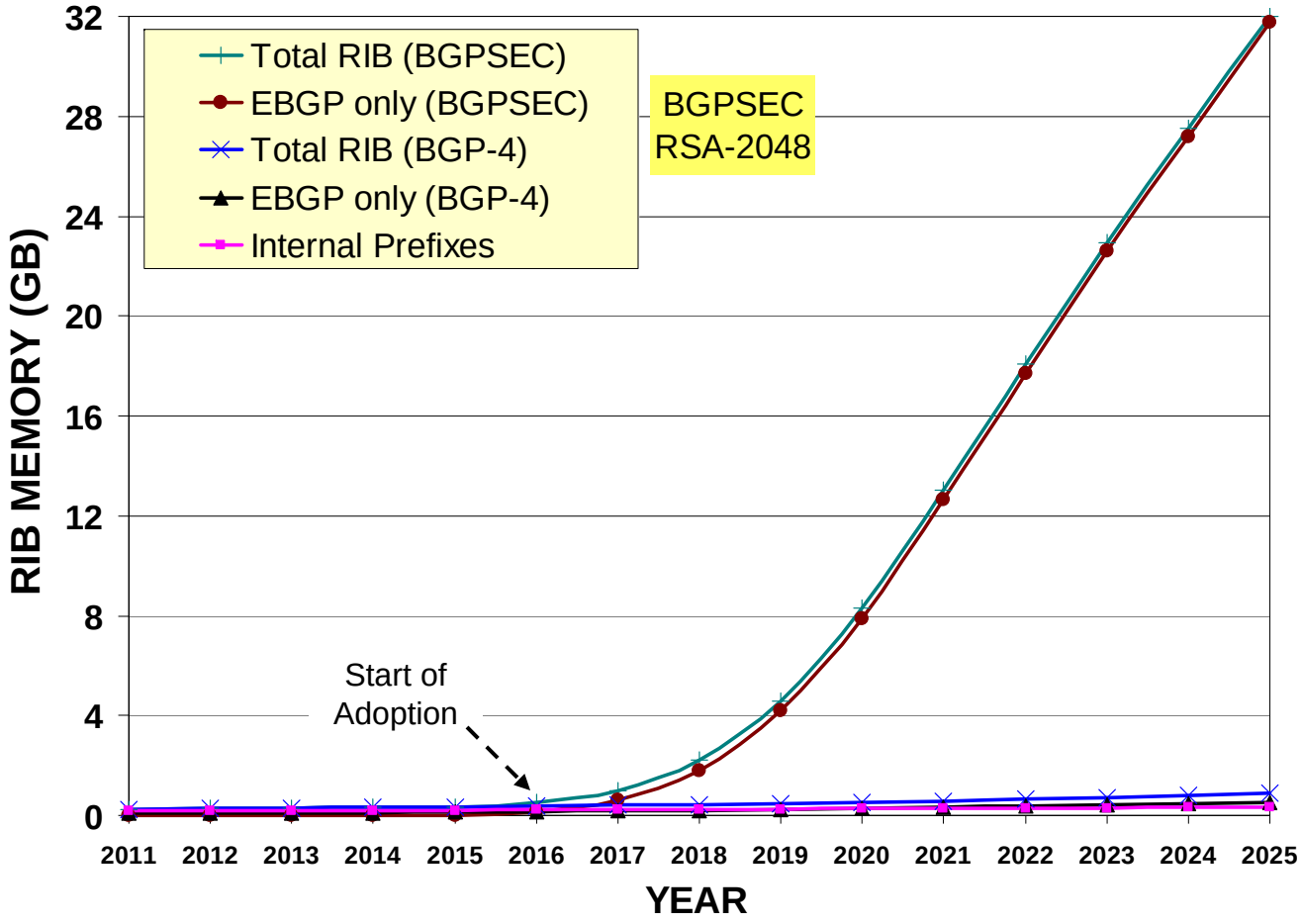
Contribution to RIB Memory due only to Signed eBGP Prefix Paths

Total # Signed eBGP Prefix-Paths in RIB	For RSA-2048 Signature Alg. (GB)	For ECDSA-256 Signature Alg. (GB)
500000	0.62	0.22
1000000	1.25	0.44
1500000	1.87	0.66
2000000	2.49	0.88
2500000	3.12	1.10
3000000	3.74	1.32
3500000	4.37	1.54
4000000	4.99	1.76
4500000	5.61	1.98
5000000	6.24	2.21
5500000	6.86	2.43
6000000	7.48	2.65
6500000	8.11	2.87
7000000	8.73	3.09
7500000	9.36	3.31
8000000	9.98	3.53
8500000	10.60	3.75
9000000	11.23	3.97
9500000	11.85	4.19
10000000	12.47	4.41
10500000	13.10	4.63
11000000	13.72	4.85
11500000	14.35	5.07
12000000	14.97	5.29
12500000	15.59	5.51
13000000	16.22	5.73

Total # Signed eBGP Prefix-Paths in RIB	For RSA-2048 Signature Alg. (GB)	For ECDSA-256 Signature Alg. (GB)
13500000	16.84	5.95
14000000	17.46	6.17
14500000	18.09	6.39
15000000	18.71	6.62
15500000	19.33	6.84
16000000	19.96	7.06
16500000	20.58	7.28
17000000	21.21	7.50
17500000	21.83	7.72
18000000	22.45	7.94
18500000	23.08	8.16
19000000	23.70	8.38
19500000	24.32	8.60
20000000	24.95	8.82
20500000	25.57	9.04
21000000	26.20	9.26
21500000	26.82	9.48
22000000	27.44	9.70
22500000	28.07	9.92
23000000	28.69	10.14
23500000	29.31	10.36
24000000	29.94	10.58
24500000	30.56	10.80
25000000	31.19	11.03
25500000	31.81	11.25
26000000	32.43	11.47

RIB Size Estimation: Relative Measure of Contributions due to eBGP & Internal Prefixes

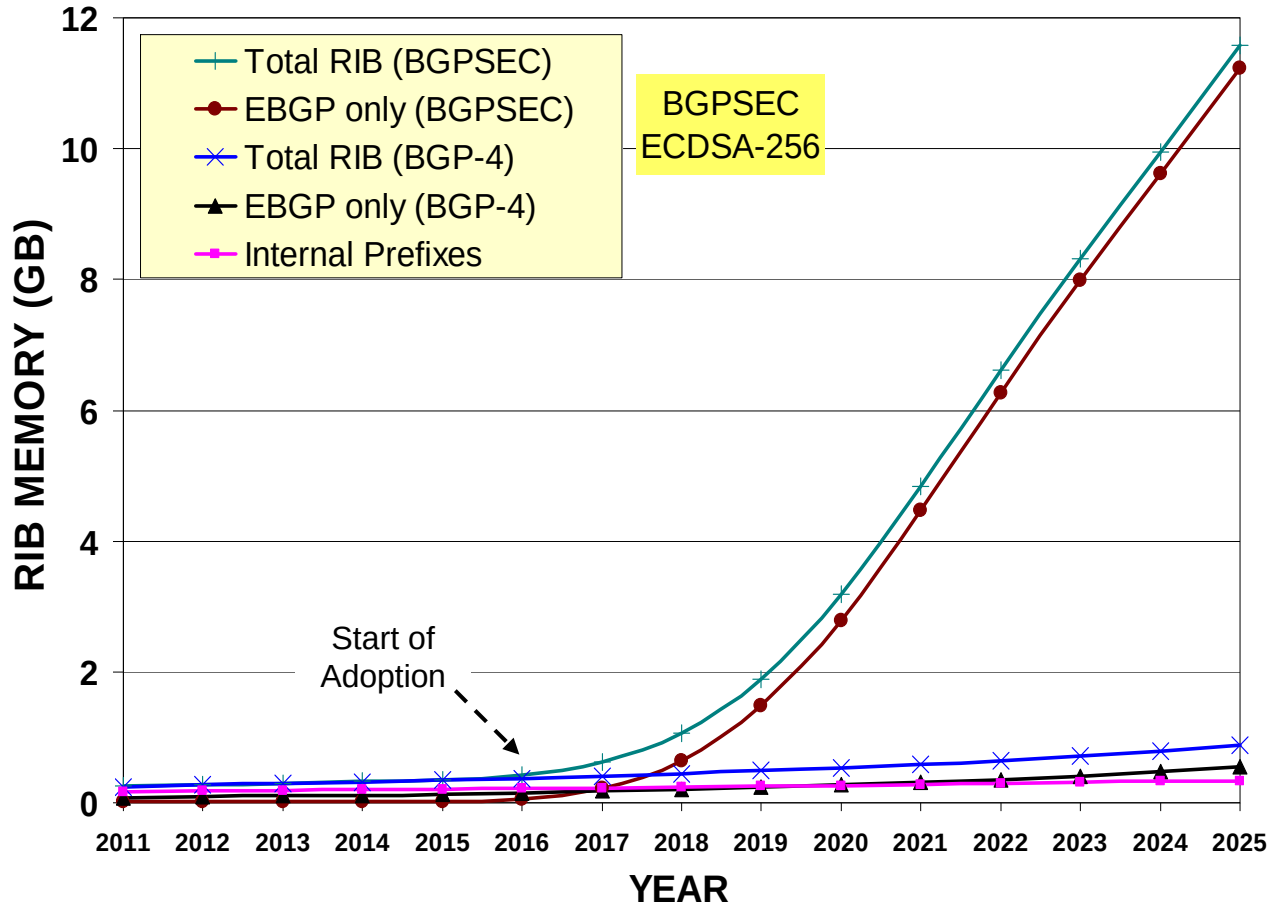
- Estimate for Route Reflector (prefix-path multiplier factor = 9.55)
- Contribution to RIB size due to internal prefixes (unsigned) is very small
- Signed eBGP prefixes dominate



RSA-2048

RIB Size Estimation: Relative Measure of Contributions due to eBGP & Internal Prefixes

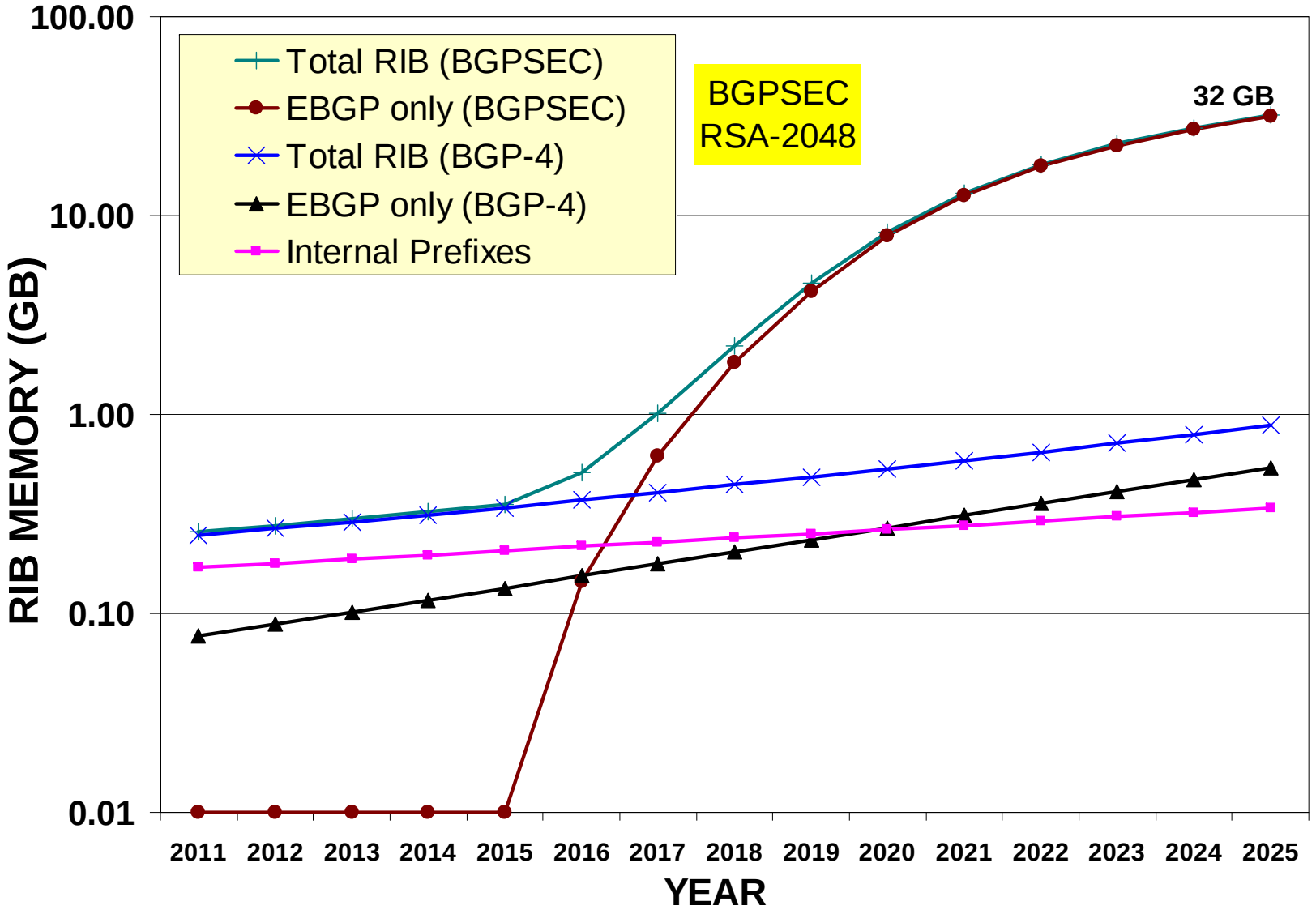
- Estimate for Route Reflector (prefix-path multiplier factor = 9.55)
- Contribution to RIB size due to internal prefixes (unsigned) is very small
- Signed eBGP prefixes dominate



ECDSA-256

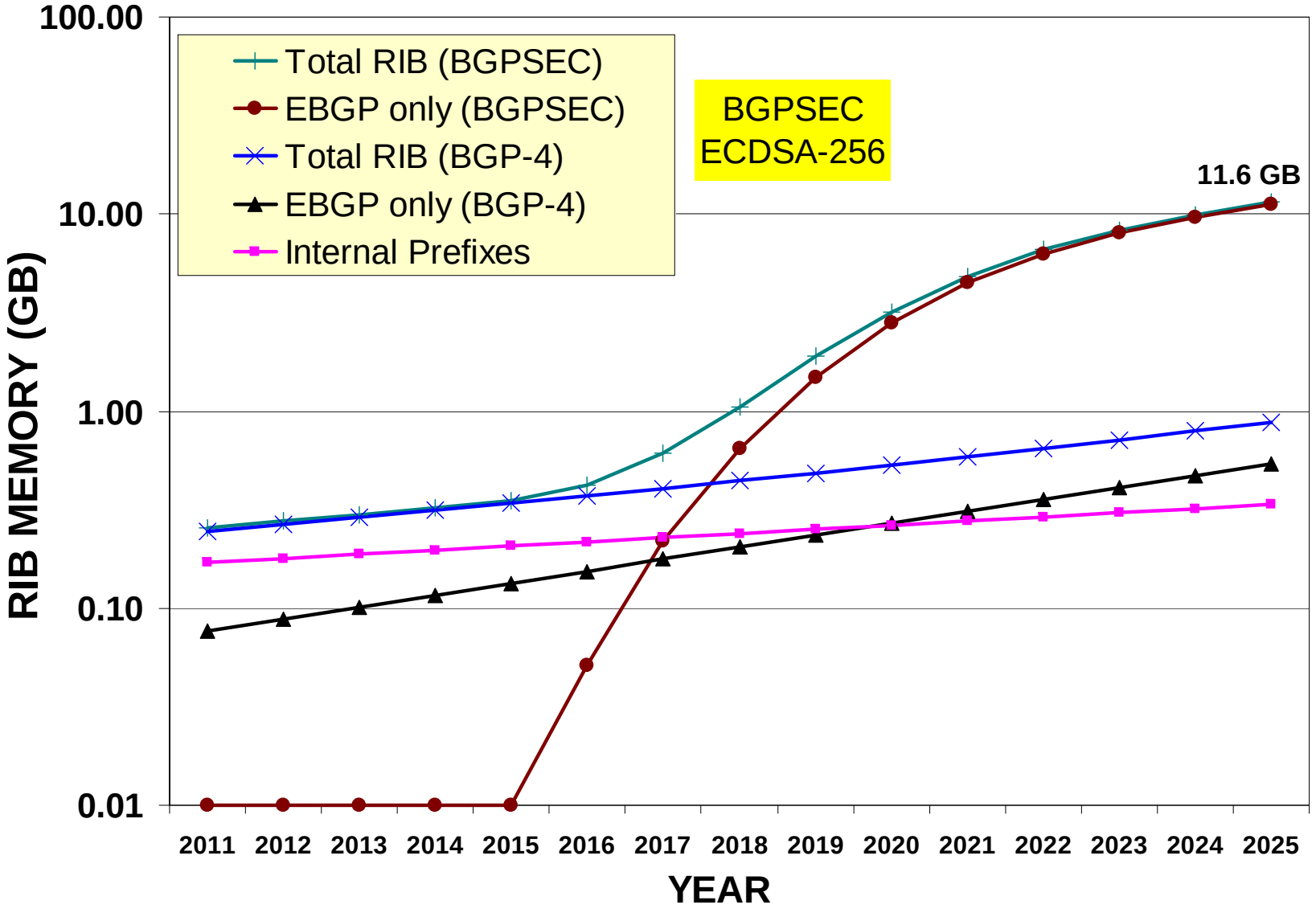
RIB Size Estimation (RSA-2048)

Same Figure as on Slide 16 but with Logarithmic Scale



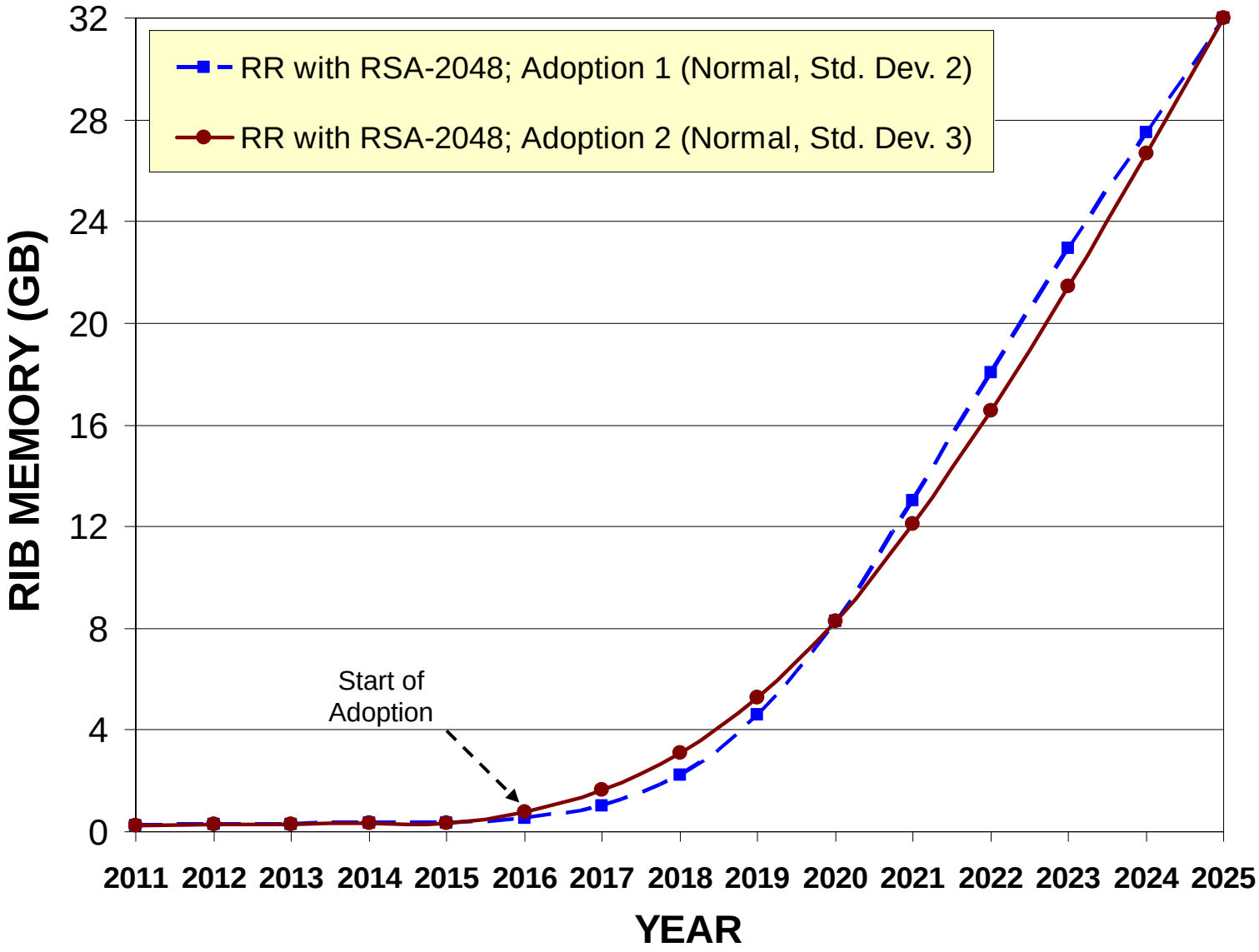
RIB Size Estimation (ECDSA-256)

Same Figure as on Slide 17 but with Logarithmic Scale



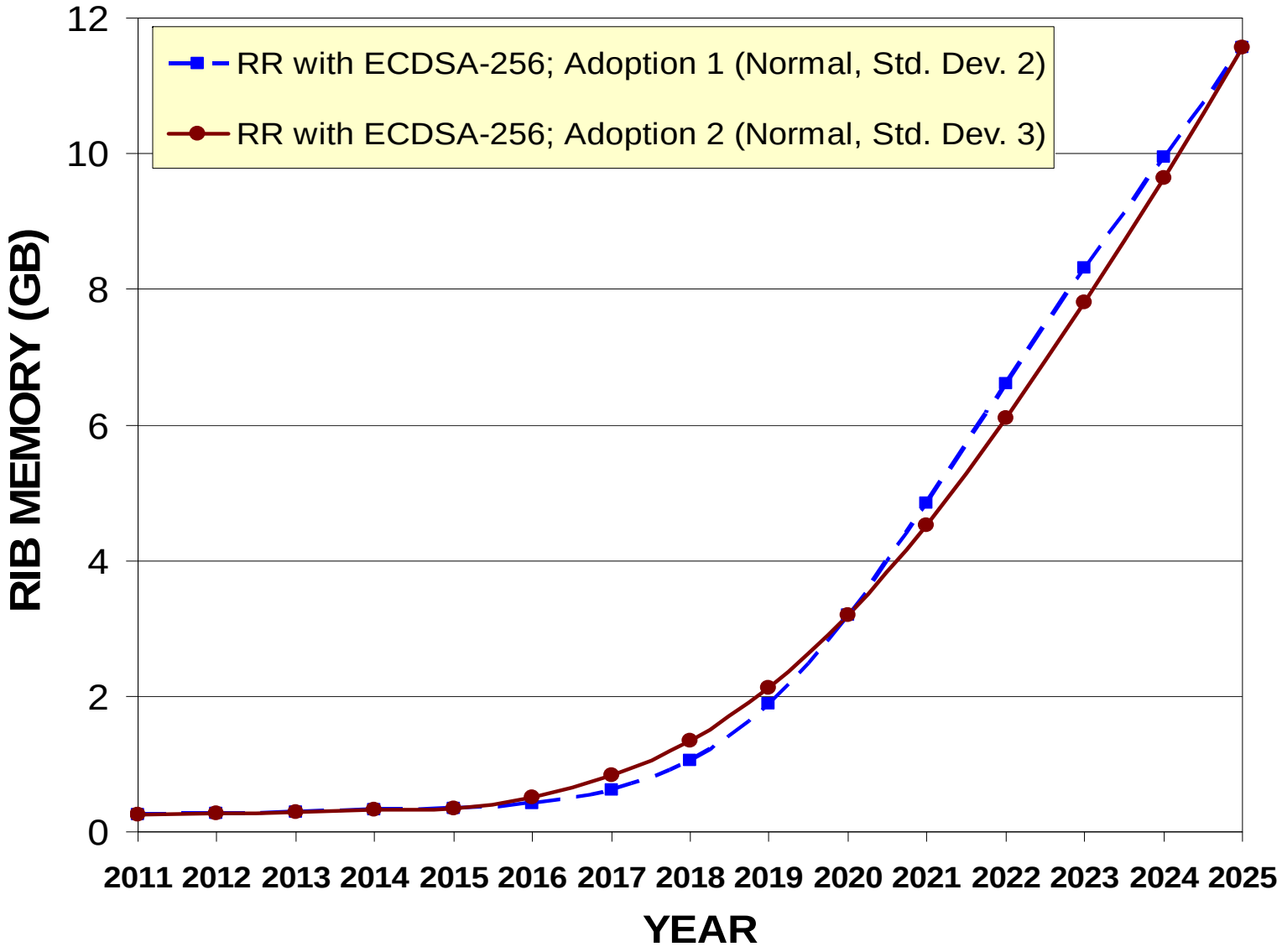
Sensitivity to Adoption Rate Model (RSA-2048)

- See Slides 7 and 8 for details of Adoption rate models 1 and 2



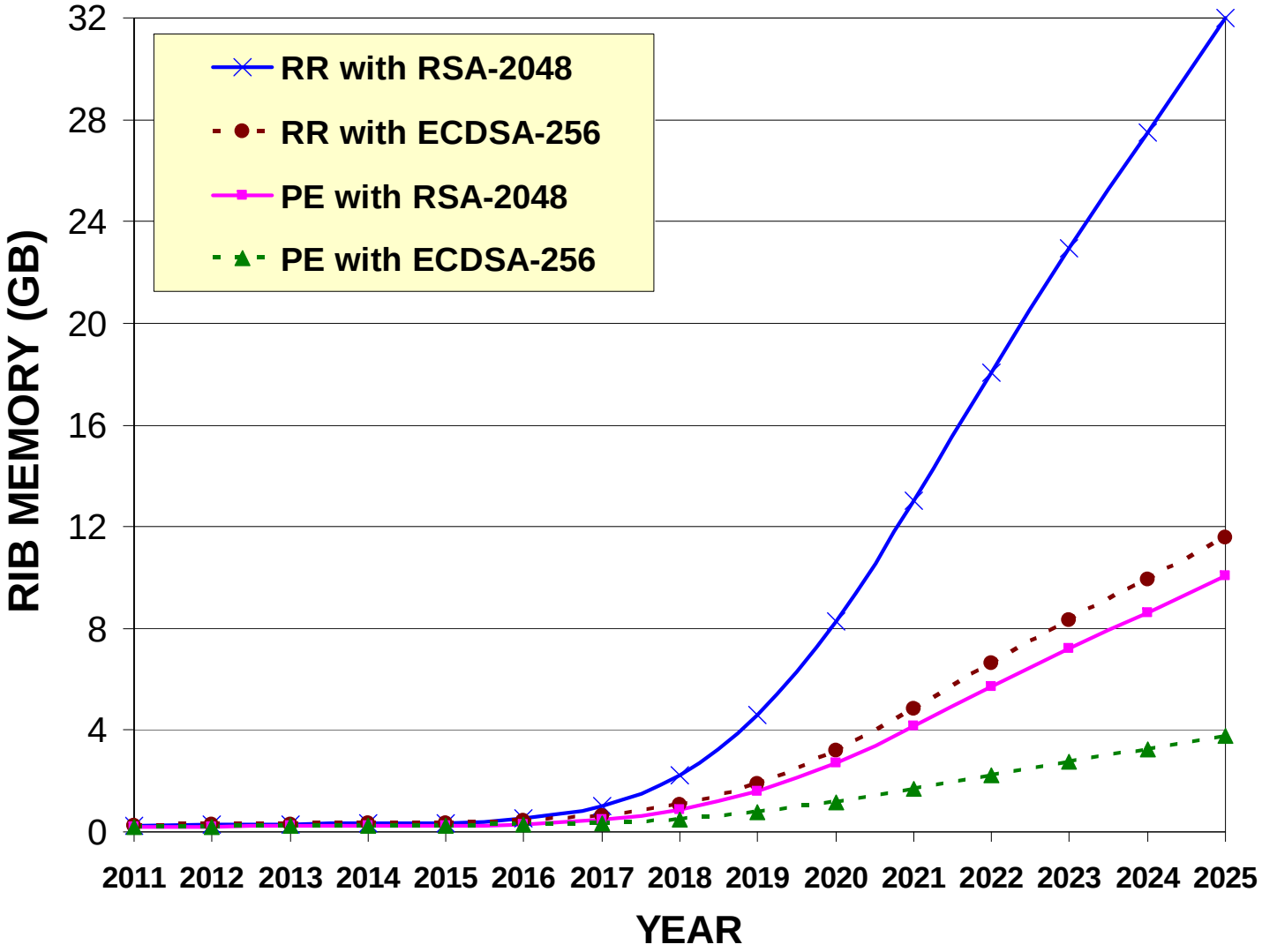
Sensitivity to Adoption Rate Model (ECDSA-256)

- See Slides 7 and 8 for details of Adoption rate models 1 and 2



RIB Size Estimation

Route Reflector / PE Router & RSA-2048 / ECDSA-256



ECDSA-256 vs. ECDSA-224

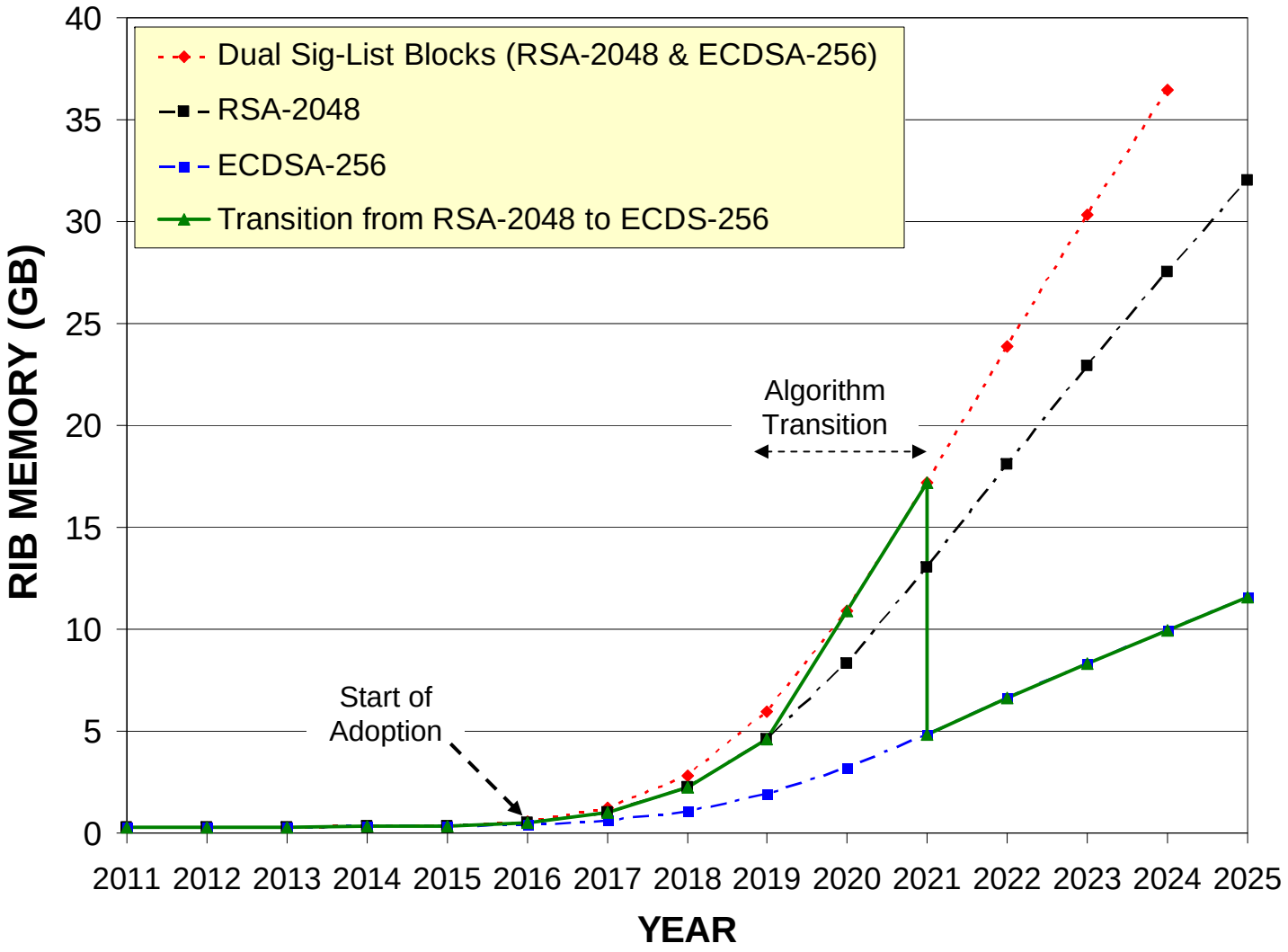
- ECDSA-224 (56 octet sig) is comparable to RSA-2048 (256 octet sig) in terms of signature strength
- But the RIB size is only slightly higher for ECDSA-256 (64 octet sig) as compared to ECDSA-224
- Might as well use ECDSA-256 and have greater longevity for sig algorithm

Year	# Internal Prefixes	# External (eBGP) prefixes	Total RIB Size for ECDSA-256	Total RIB Size for ECDSA-224
2011	800000	377000	0.26	0.26
2012	840000	433550	0.28	0.28
2013	882000	498583	0.30	0.30
2014	926100	573370	0.32	0.32
2015	972405	659375	0.35	0.35
2016	1021025	758282	0.42	0.42
2017	1072077	872024	0.61	0.60
2018	1125680	1002827	1.05	1.01
2019	1181964	1153252	1.89	1.78
2020	1241063	1326239	3.19	2.98
2021	1303116	1525175	4.84	4.50
2022	1368271	1753952	6.61	6.13
2023	1436685	2017044	8.32	7.71
2024	1508519	2319601	9.94	9.21
2025	1583945	2667541	11.57	10.72

- Estimates for Route Reflector (prefix-path multiplier factor = 9.55)

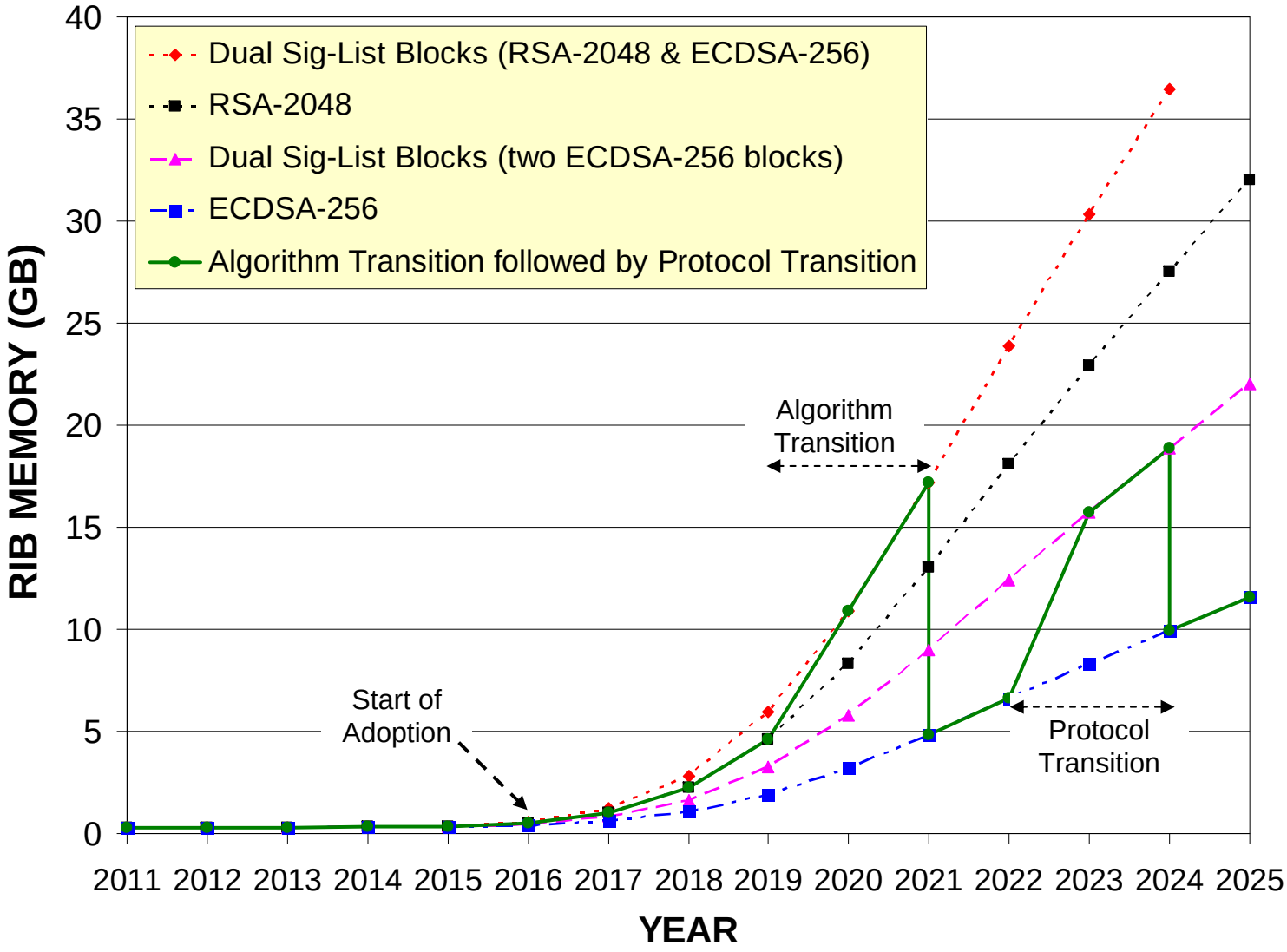
BGPSEC Signature Algorithm Transition (Example)

- Dual signature-list blocks are used during algorithm transition (see draft-lepinski-bgpsec-protocol)



BGPSEC Signature Algorithm Transition Followed by Protocol Transition (Example)

- Dual signature-list blocks are also used during protocol/alg transition (see draft-lepinski-bgpsec-protocol)



Summary & Conclusions

- RIB sizes have been estimated for realistic RR and PE scenarios (with input from a large, Tier 1 ISP)
- Different signature algorithms considered (RSA-2048, ECDSA-256)
- RIB memory needs to be engineered so it is adequate for algorithm/protocol transition down the road
- 15% yearly growth for unique eBGP prefixes (377K in 2011 to 2.7M in 2025)
- BGPSEC adoption curve – truncated Normal distribution
- 9.55x multiplier applied to determine # prefix paths in RR
- RIB memory requirement of 0.5GB in 2016 to 8.3 GB in 2020 to 32 GB in 2025 (worst case assuming RSA-2048 all the way)
- Algorithm transition to ECDSA-256 likely (should happen) before 2020
- Assuming such transition, 20 GB for RIB memory would be a conservative estimate -- good all the way out to 2025 (Slide 25)