RIB Size Estimation for BGPSEC

K. Sriram

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

IETF-81 SIDR WG Meeting

July 28, 2011

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

Acknowledgements: Many thanks are due to the BGPSEC Design Team for comments and suggestions. Thanks are also due to people in the SIDR WG who have shared measurement data, made suggestions, or critiqued the work.

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.

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

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

Reference: draft-sidr-bgpsec-protocol

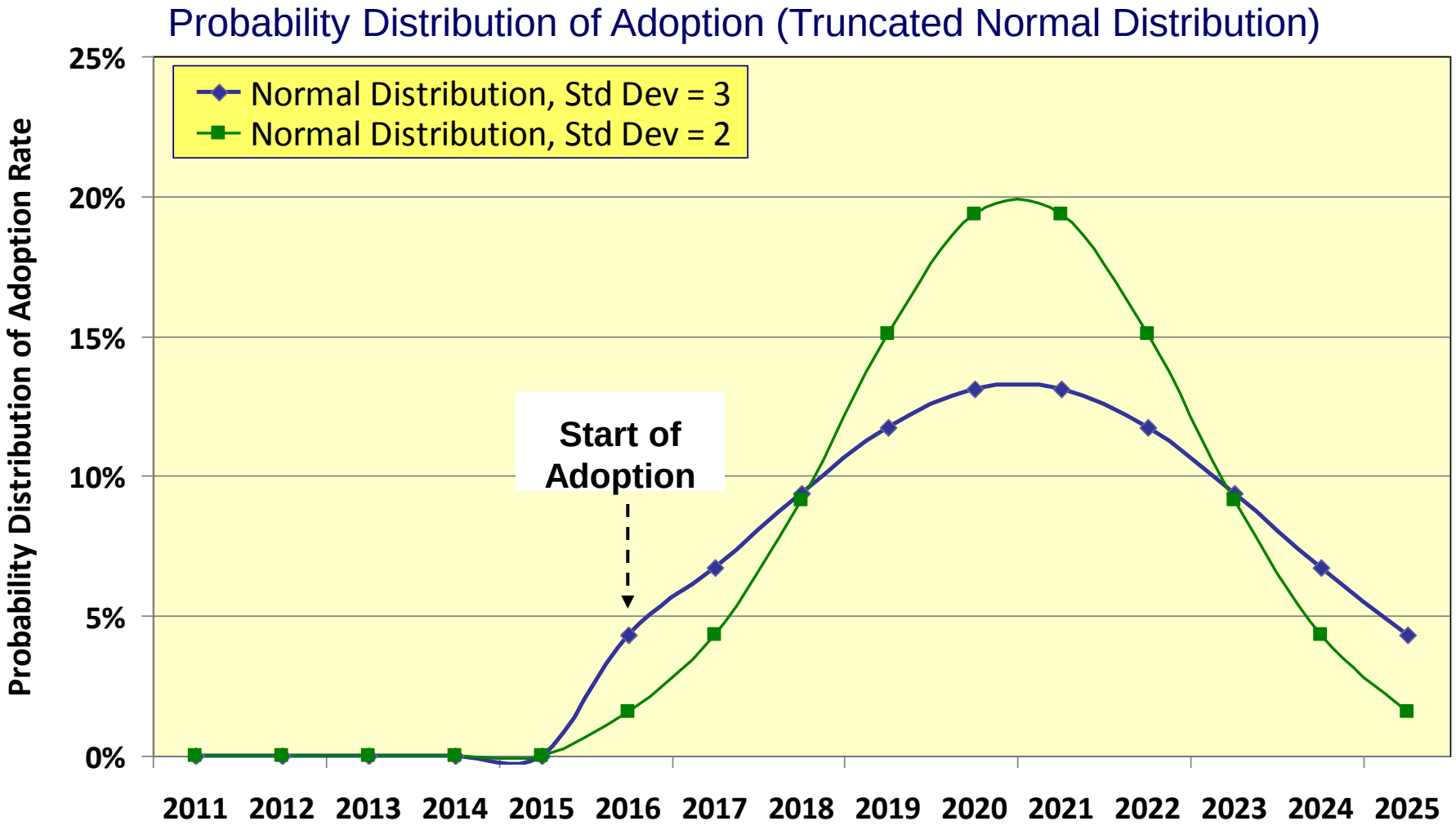
Estimation of BGPSEC Update Sizes

BGPSEC Signed Update Size:	IPv4 (octets)	IPv6 (octets)
For RSA-2048 Signatuer Alg	1188	1200
For ECDSA-256 Signatuer Alg	420	432

Unsigned Update	78	90
RIB memory storage ovehead	5.0%	5.0%

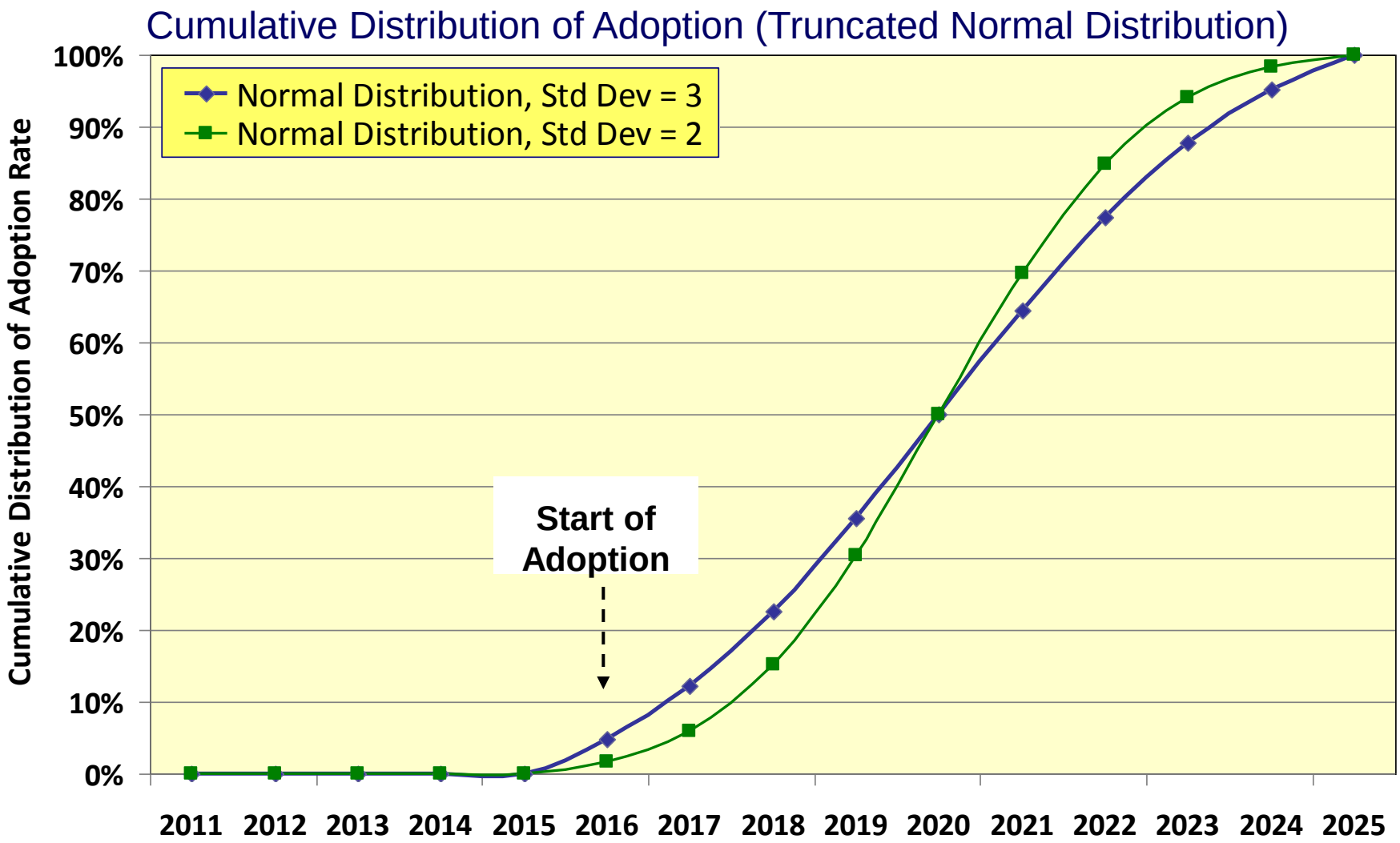
- It should also be noted that eBGP updates in BGP-4 average 3.83 prefixes per update whereas the same in BGPSEC have only a single prefix per update (un-optimized).
- Unsigned update size was measured from Routeviews data.
- Signed update sizes are estimated (see the excel spread sheet for details: http://www.antd.nist.gov/~ksriram/BGPSEC_RIB.xls).

BGPSEC Adoption Rate (1)



- In the RIB estimates that follow, we will apply truncated Normal distribution of adoption with Std. Deviation = 2 (Green plot).

BGPSEC Adoption Rate (2)



- In the RIB estimates that follow, we will apply truncated Normal distribution of adoption with Std. Deviation = 2 (Green plot).

PE Router RIB Size Estimation for BGPSEC

			PE Router			PE Router		Contribution to RIB Memory Due to IPv4 and IPv6 eBGP Updates in PE Router	
Year	IPv4 Growth Rate	# Unique IPv4 eBGP Prefixes (FIB)	Total # Signed IPv4 eBGP Prefix-Paths in RIB	IPv6 Growth Rate	# Unique IPv6 eBGP Prefixes (FIB)	Total # Signed IPv6 eBGP Prefix-Paths in RIB	BGPSEC Adoption (% Prefix-Paths Signed)	For RSA-2048 Signature Alg. (GB)	For ECDSA-256 Signature Alg. (GB)
2011	12%	377000	1100840	100%	4000	11680	0%	0.09	0.09
2012	12%	422240	1232941	90%	8000	23360	0%	0.10	0.10
2013	12%	472909	1380894	80%	15200	44384	0%	0.12	0.12
2014	12%	529658	1546601	70%	27360	79891	0%	0.13	0.13
2015	12%	593217	1732193	60%	46512	135815	0%	0.15	0.15
2016	12%	664403	1940056	50%	74419	217304	2%	0.22	0.19
2017	12%	744131	2172863	40%	111629	325956	6%	0.38	0.26
2018	12%	833427	2433607	30%	156280	456339	15%	0.75	0.40
2019	12%	933438	2725639	30%	203164	593240	30%	1.46	0.64
2020	12%	1045451	3052716	30%	264114	771212	50%	2.55	1.01
2021	12%	1170905	3419042	30%	343348	1002576	70%	3.96	1.48
2022	12%	1311413	3829327	30%	446352	1303348	85%	5.51	2.00
2023	12%	1468783	4288846	30%	580258	1694353	94%	7.07	2.53
2024	12%	1645037	4803508	30%	754335	2202659	98%	8.64	3.08
2025	12%	1842441	5379929	30%	980636	2863457	100%	10.32	3.67

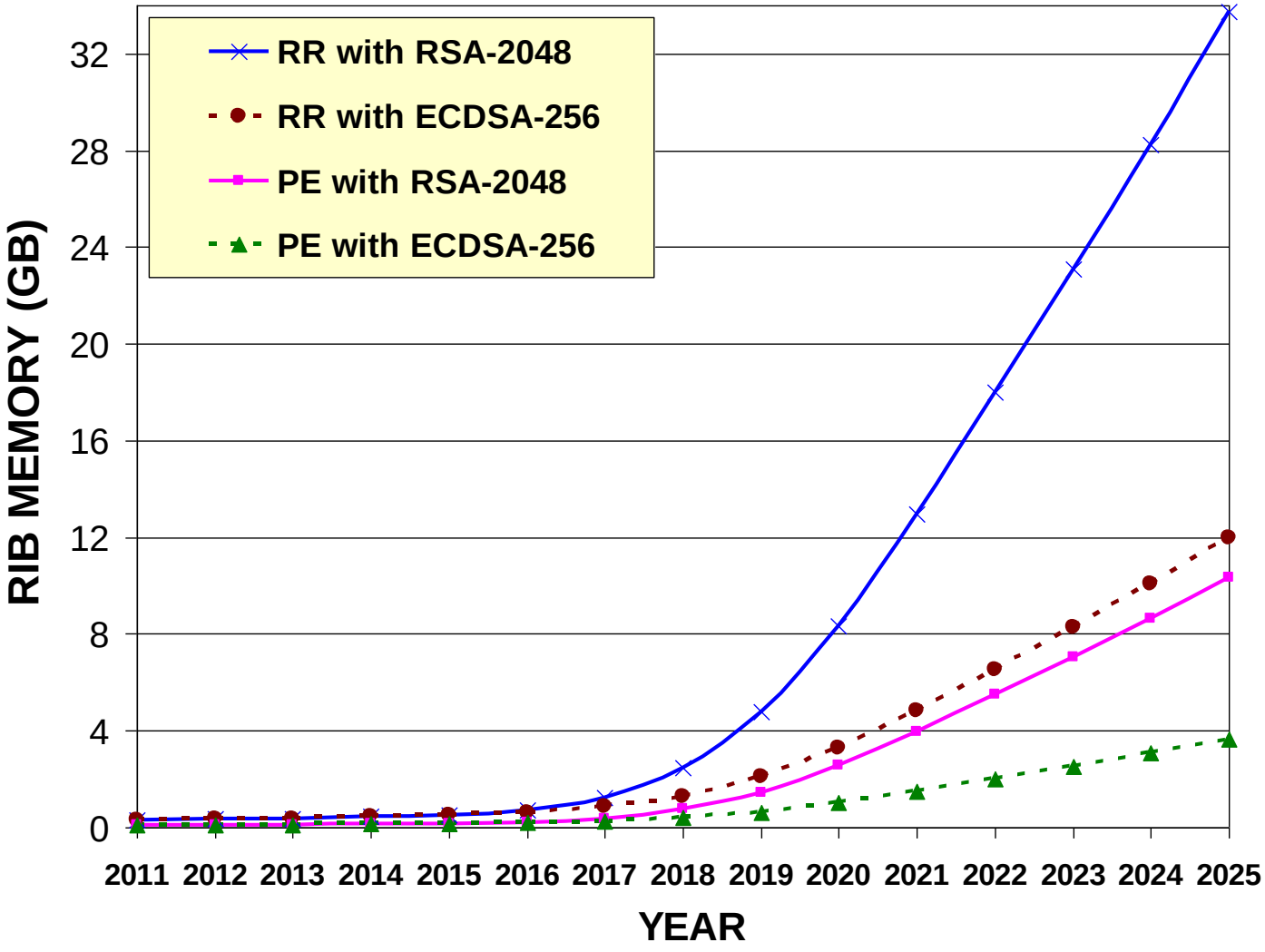
- Geoff Huston's IPv4 data shows a steady 12% (approximately) yearly growth rate for eBGP IPv4 prefixes over the past few years (2008-2011). http://bgp.potaroo.net/index-bgp.html
- His data also shows 4000 announced IPv6 at start of 2011 with about 100% growth rate so far in 2011.

Route Reflector RIB Size Estimation for BGPSEC

			Route Reflector			Route Reflector		Contribution to RIB Memory Due to IPv4 and IPv6 eBGP Updates in Route Reflector	
Year	IPv4 Growth Rate	# Unique IPv4 eBGP Prefixes (FIB)	Total # Signed IPv4 eBGP Prefix-Paths in RIB	IPv6 Growth Rate	# Unique IPv6 eBGP Prefixes (FIB)	Total # Signed IPv6 eBGP Prefix-Paths in RIB	BGPSEC Adoption (% Prefix-Paths Signed)	For RSA-2048 Signature Alg. (GB)	For ECDSA-256 Signature Alg. (GB)
2011	12%	377000	3600350	100%	4000	38200	0.00%	0.30	0.30
2012	12%	422240	4032392	90%	8000	76400	0.00%	0.34	0.34
2013	12%	472909	4516279	80%	15200	145160	0.00%	0.38	0.38
2014	12%	529658	5058233	70%	27360	261288	0.00%	0.44	0.44
2015	12%	593217	5665220	60%	46512	444190	0.00%	0.51	0.51
2016	12%	664403	6345047	50%	74419	710703	1.61%	0.72	0.63
2017	12%	744131	7106453	40%	111629	1066055	5.97%	1.25	0.86
2018	12%	833427	7959227	30%	156280	1492477	15.21%	2.47	1.31
2019	12%	933438	8914334	30%	203164	1940220	30.44%	4.76	2.10
2020	12%	1045451	9984054	30%	264114	2522286	50.00%	8.34	3.30
2021	12%	1170905	11182141	30%	343348	3278972	69.56%	12.95	4.84
2022	12%	1311413	12523997	30%	446352	4262664	84.79%	18.02	6.54
2023	12%	1468783	14026877	30%	580258	5541463	94.03%	23.12	8.28
2024	12%	1645037	15710102	30%	754335	7203902	98.39%	28.24	10.06
2025	12%	1842441	17595315	30%	980636	9365072	100.00%	33.75	12.01

- Please see notes on previous slides.

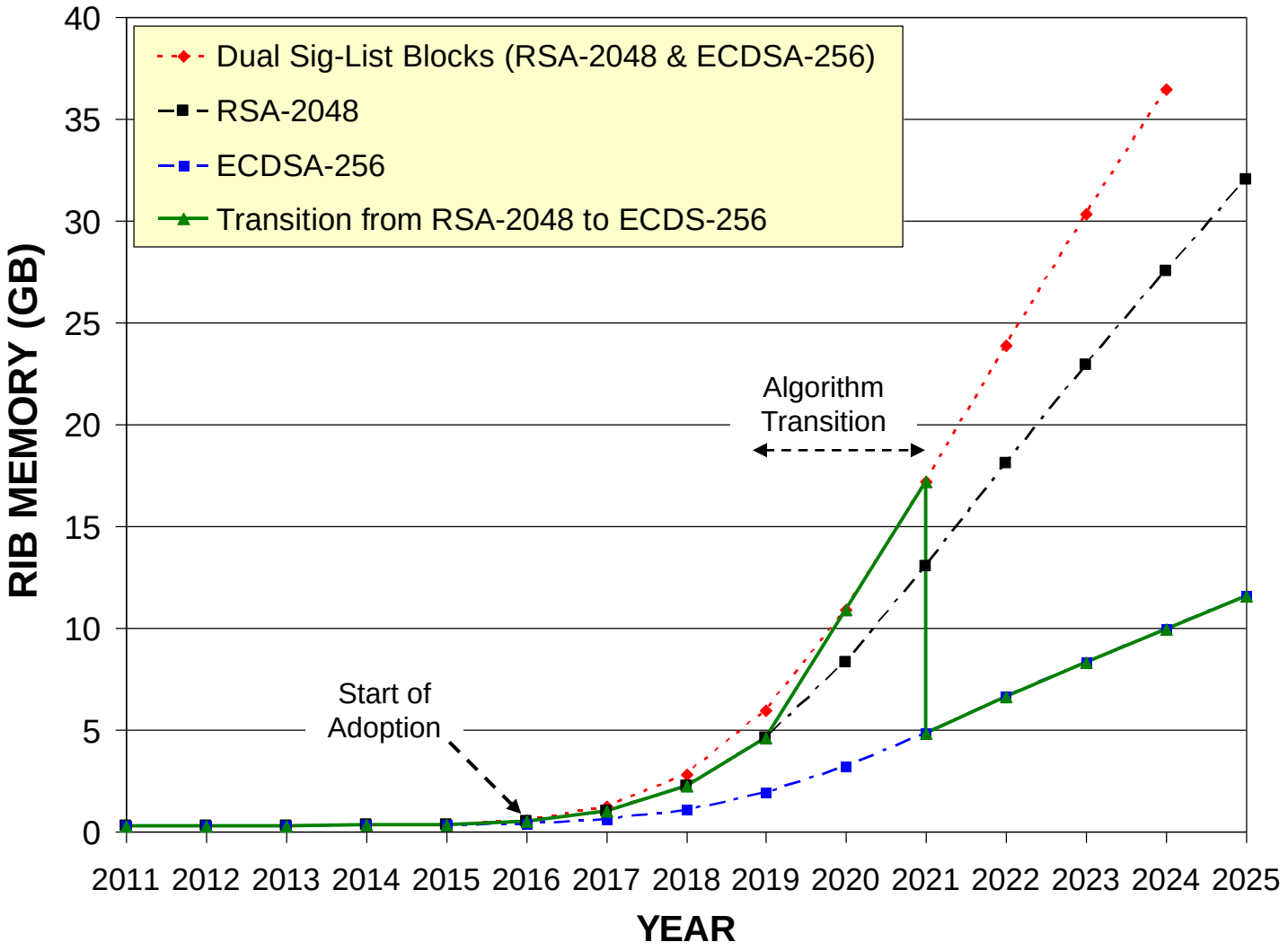
Comparison: RSA-2048 vs. ECDSA-256



- Includes IPv4 and IPv6 prefixes.
- See slides 7, 8 for details.

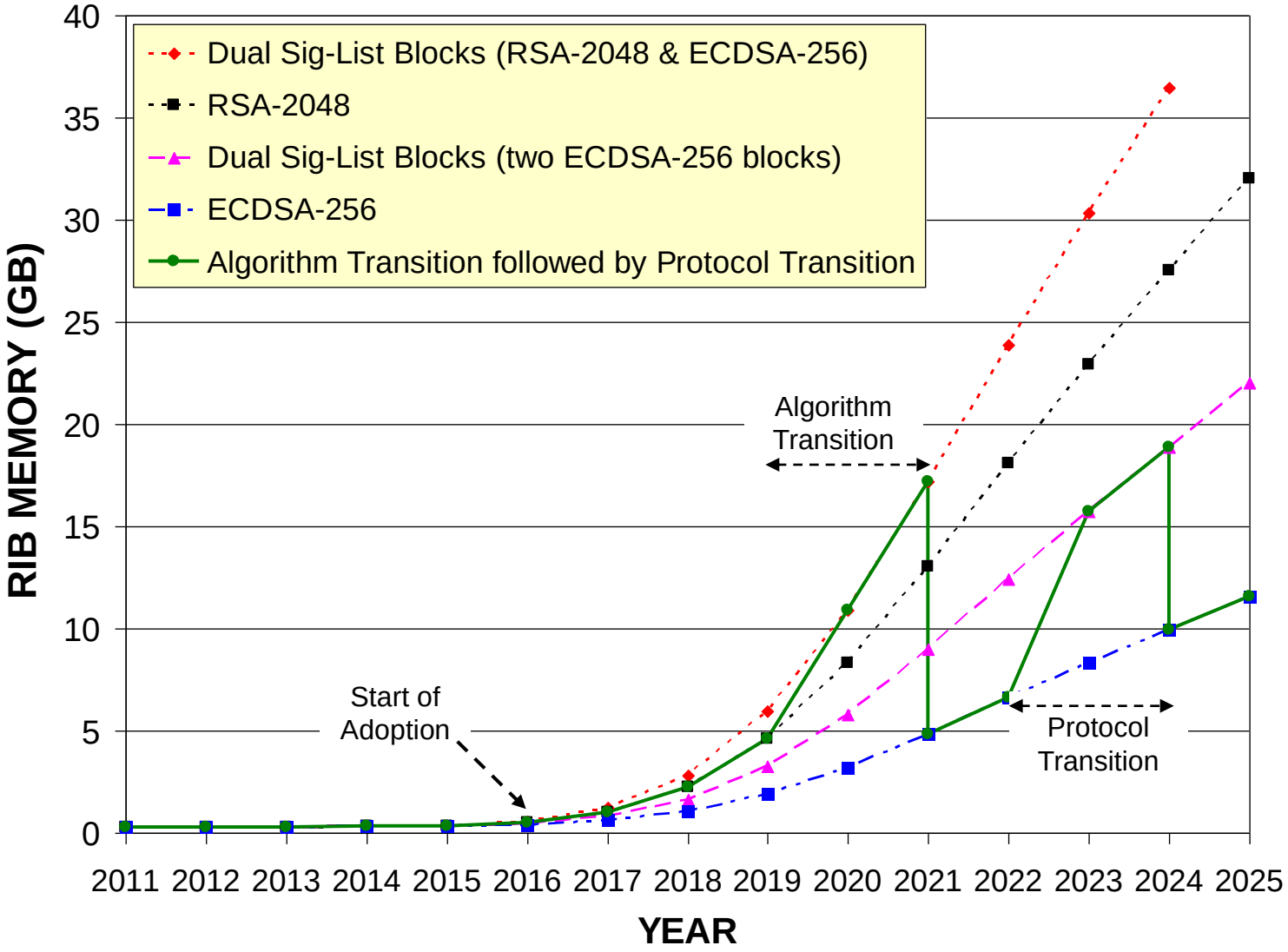
BGPSEC Signature Algorithm Transition (Example)

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



BGPSEC Signature Algorithm Transition Followed by Protocol Transition (Example)

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



Summary & Conclusions

- RIB sizes have been estimated for realistic RR and PE scenarios (with input from a large, Tier 1 ISP and also from Geoff Huston's latest measurement data for eBGP IPv6 and IPv4 prefixes http://bgp.potaroo.net/index-bgp.html)
- Signature algorithms considered: RSA-2048 and ECDSA-256
- RIB memory needs to be engineered so it is adequate for algorithm/protocol transition down the road
- Please also see previously shared slides http://www.antd.nist.gov/~ksriram/BGPSEC_RIB_Estimation.pdf for other related details and discussion regarding the modeling
- The excel spread sheet is made available so anyone can play with assumptions in accordance with their view. Several details of the modeling can be gleaned from the excel spread sheet as well: http://www.antd.nist.gov/~ksriram/BGPSEC_RIB.xls
- Thanks for the discussion and comments on the SIDR list so far. Further comments/suggestions are very welcome