

Evaluating the Performance Impact of PKI on BGP Security

Meiyuan Zhao, Sean Smith
Dartmouth College

David Nicol
University of Illinois at Urbana-Champaign



Outline

- Overview
 - BGP
 - S-BGP's PKIs and attestations
 - Improved schemes
 - OA, S-A, and SAS
 - Performance evaluation
 - Simulation methodology
 - Experiment results
 - Related work
 - Conclusions and future work
-



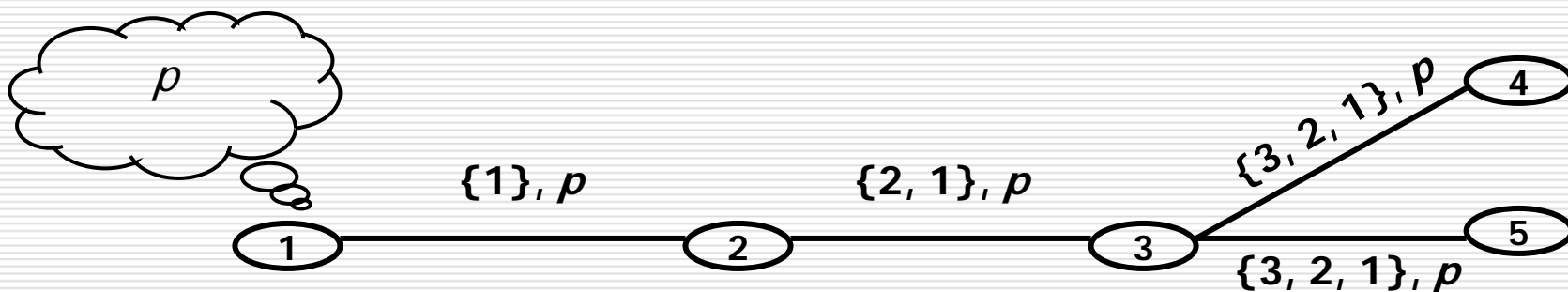
Border Gateway Protocol (BGP)

- ❑ Inter-domain routing protocol
- ❑ Mainly between autonomous systems (ASes)
- ❑ Updates are in form of route announcements

(AS_PATH, prefix)

A sequence of AS numbers
e.g., "500 300 100"

A range of IP addresses (prefix)
e.g., 129.170.0.0/16





Secure BGP (S-BGP)



Route Attestations (RAs)

Address Attestations (AAs)

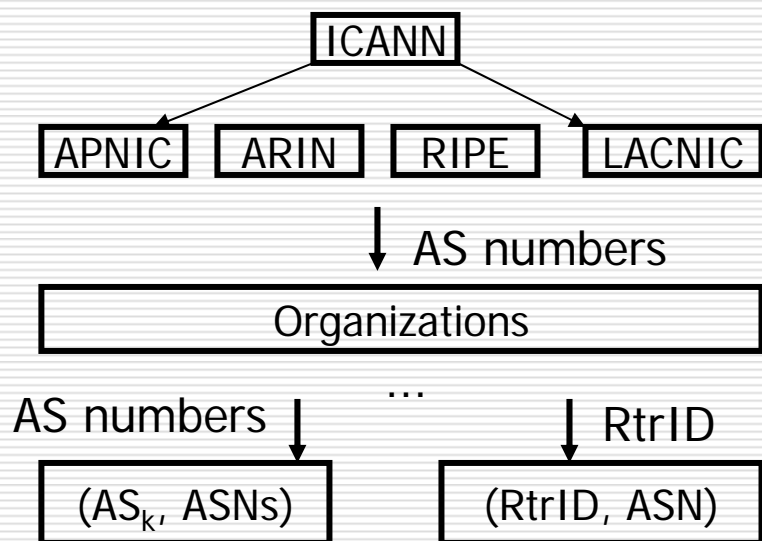
- IP address owners create AAs
 - X.509 Certificates for IP address allocation
 - $(\text{prefix}_1, \dots, \text{prefix}_k, \text{org}_y)$ address assignment
 - Routers create RAs
 - X.509 Certificates for AS# and Routers
 - $(\text{AS}, \text{AS}\#, \text{PK})$ binding
 - $(\text{RtrID}, \text{AS}\#, \text{PK})$ binding
-



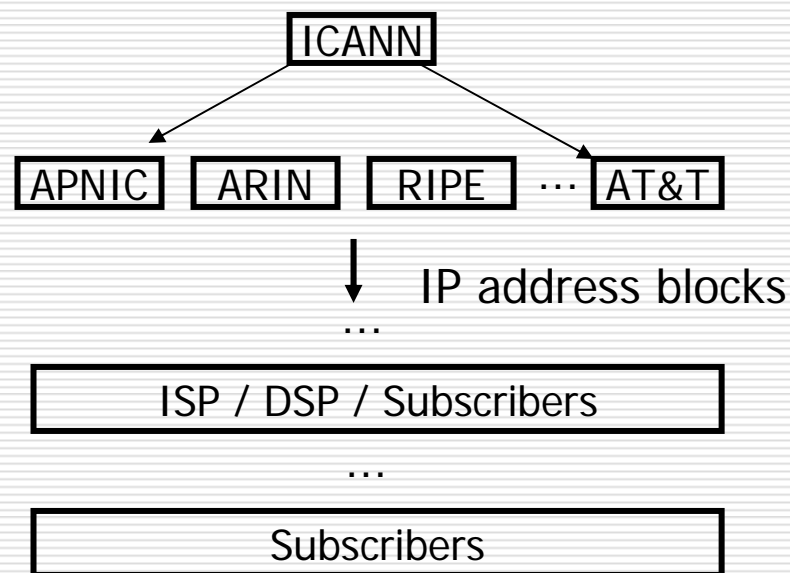
S-BGP PKIs

□ Match existing infrastructures

AS number assignment &
Binding a Router to an AS



IP Address Allocation





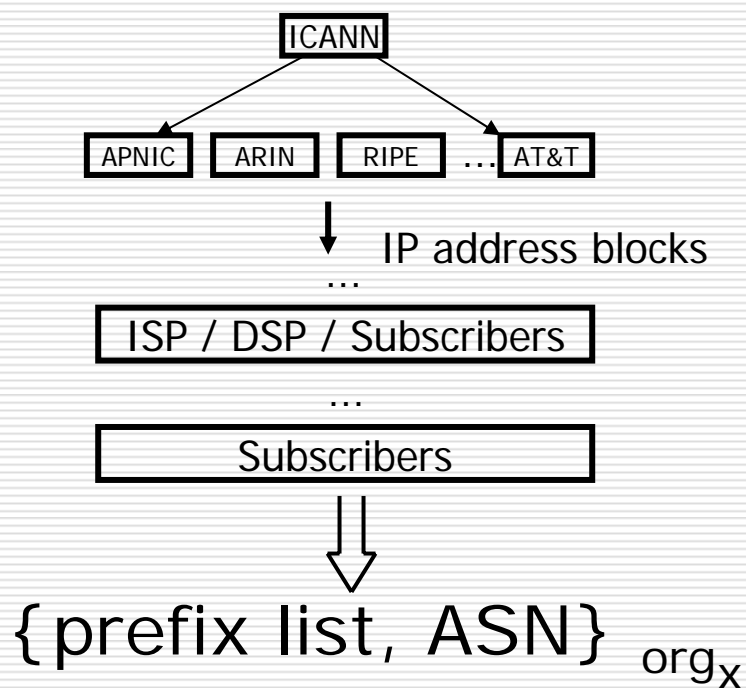
Certificate Distribution

- Scale
 - 197,709 active prefixes
 - 19,357 unique ASes
 - >50,000 organizations
 - BGP Update message MTU: 4KB
 - S-BGP X.509 Certificates: 600 bytes
 - Store certificates/CRLs locally
 - >200MB
-



S-BGP Address Attestations (AAs)

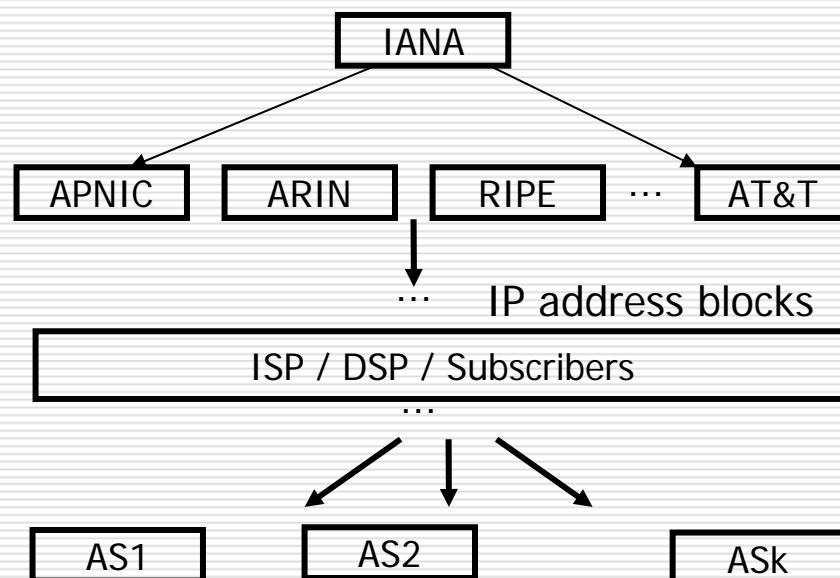
- ❑ Authorize ASes to originate routes
- ❑ CAs prepare and distribute AAs
- ❑ Long-lived, need revocation





Origin Authentication (OA)

- Short-lived attestations
- Possible in-band transmission for address delegation paths
- Variants



- OA-Simple $\{(p, \text{org})\}_K$
- OA-List $\{(p_1, \text{org}_1), (p_2, \text{org}_2), \dots, (p_i, \text{org}_i)\}_K$
- **OA-AS-List** $\{(p_1, p_2, \dots, p_k, \text{org})\}_K$
- OA-Tree Merkle hash tree, leaves: (p_i, org_i)



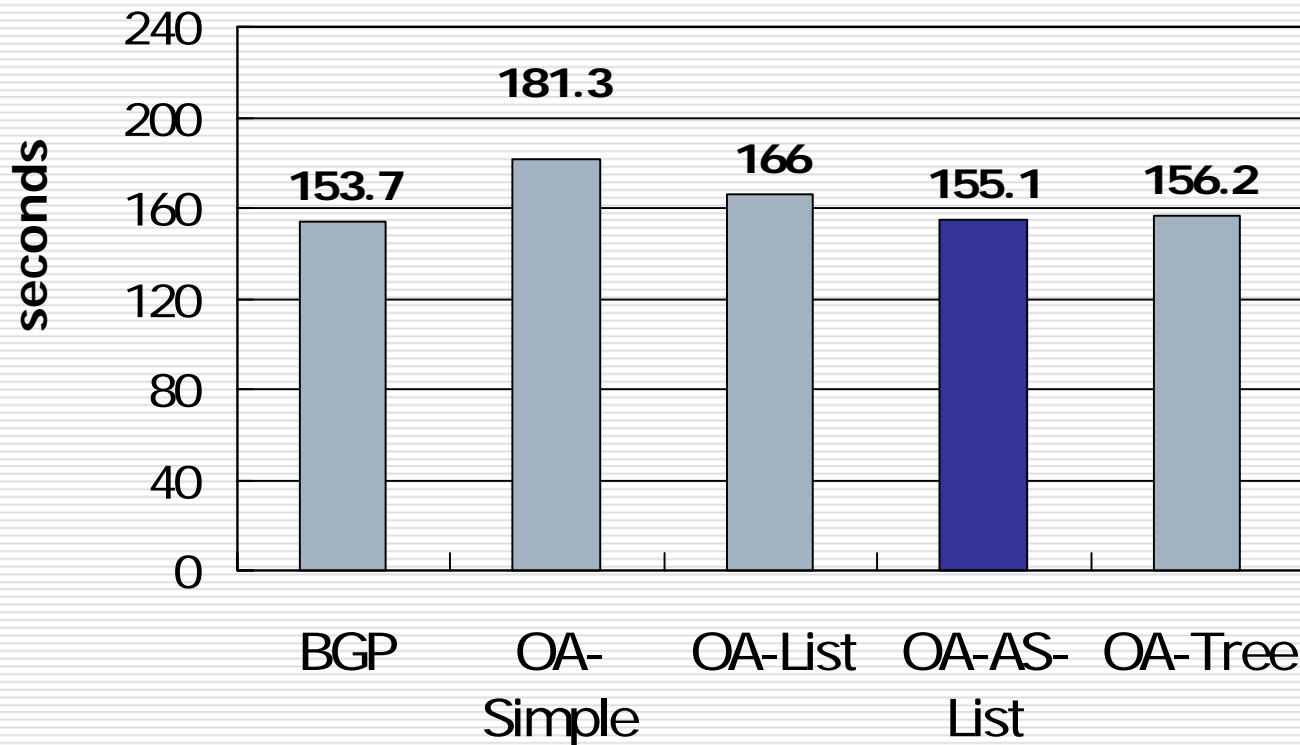
Evaluation Methodology

- AS-level network simulation—110 ASes
 - BGP router under stress—router reboot
 - PKI model
 - ASes, Routers, Organizations, CAs, Directories, and OCSP responders
 - Routers trust the roots, and OCSP responders; may trust other CAs as well
 - Check certificate revocation status
 - OCSP—sequential or parallel requests
 - CRLs (fetch fresh copies)
 - Reduced OA approximate delegation graph
 - Metrics
 - Speed—**BGP convergence time**
 - Memory
 - Message Size
-



OA Signature Performance—Convergence

- Slight slow down convergence time





OA Signature Performance—Storage

- ❑ Different costs on memory and message size
- ❑ OA-AS-List is most efficient
- ❑ Possible in-band transmission

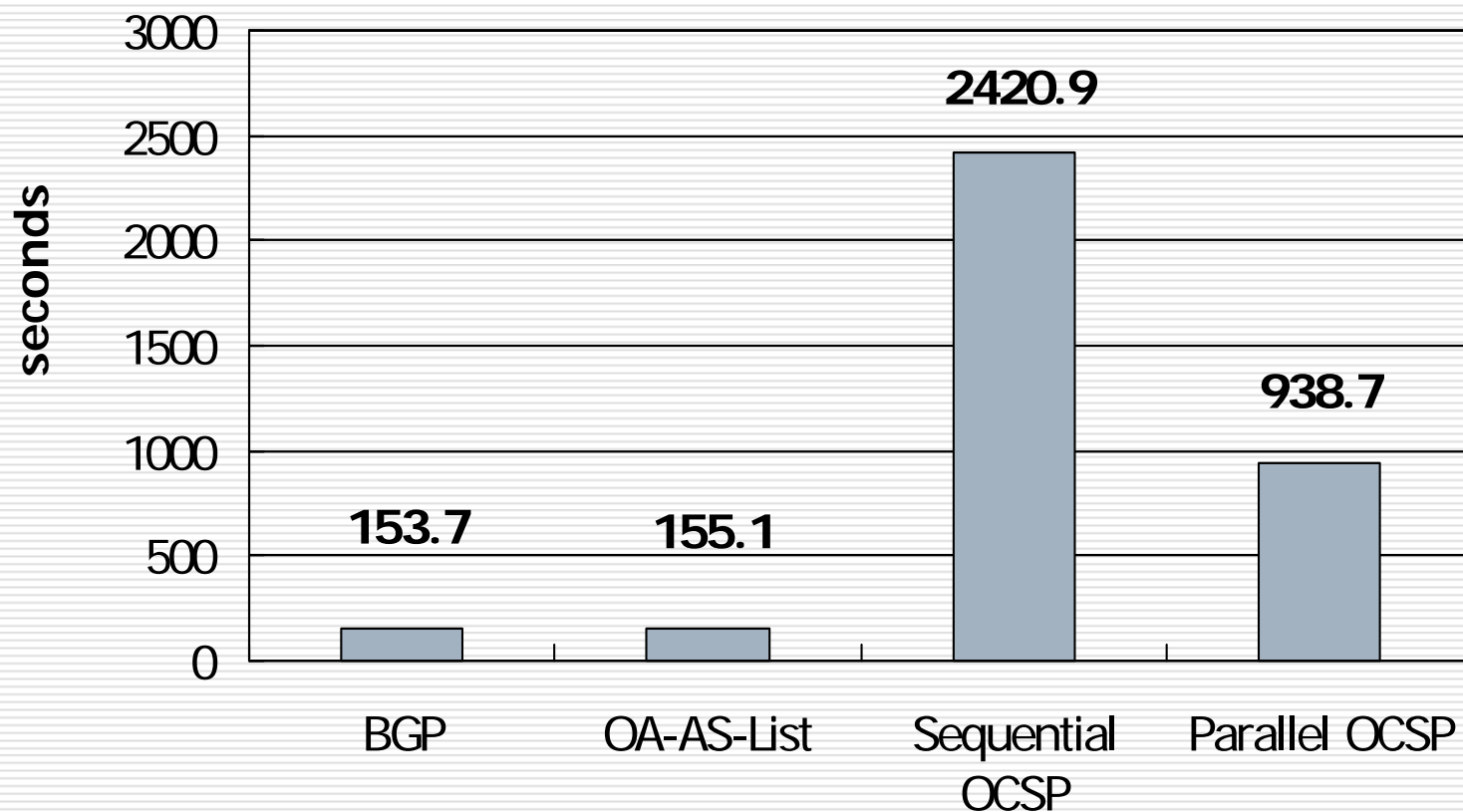
Attestation Constructions	Memory for Attestations (KB)	Message Size (Bytes)
OA-Simple	42.80	496.97
OA-List	666.27	36293.37
OA-AS-List	13.23	575.35
OA-Tree	30.22	1029.24



OA Performance—OCSP requests

□ \approx 68,000 OCSP requests

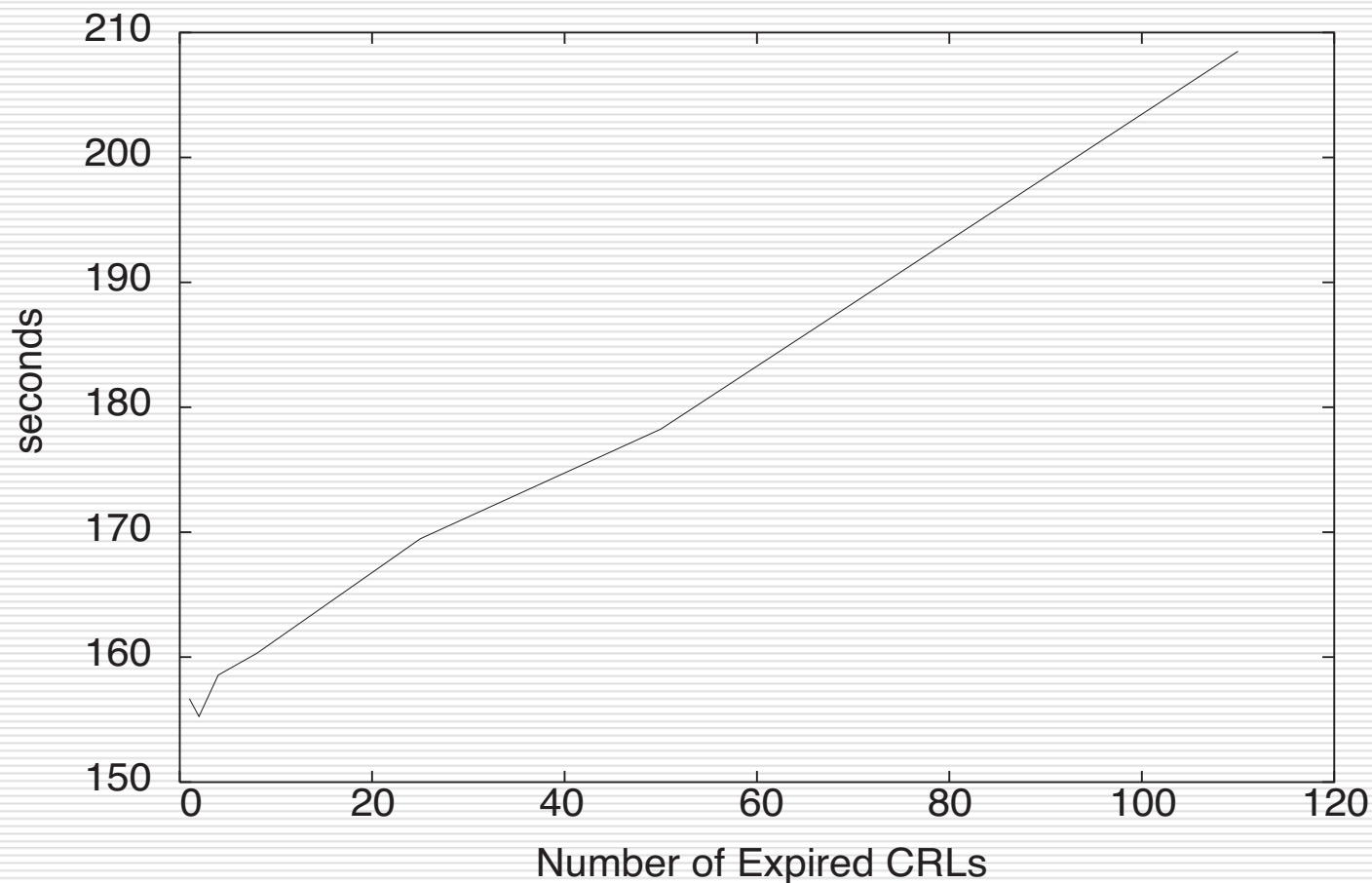
Convergence Time of OCSP Requests





OA Performance—CRLs fetching

Convergence Time of CRL Fetching





Secure BGP (S-BGP)

AS path	Prefix
---------	--------

Route Attestations (RAs)

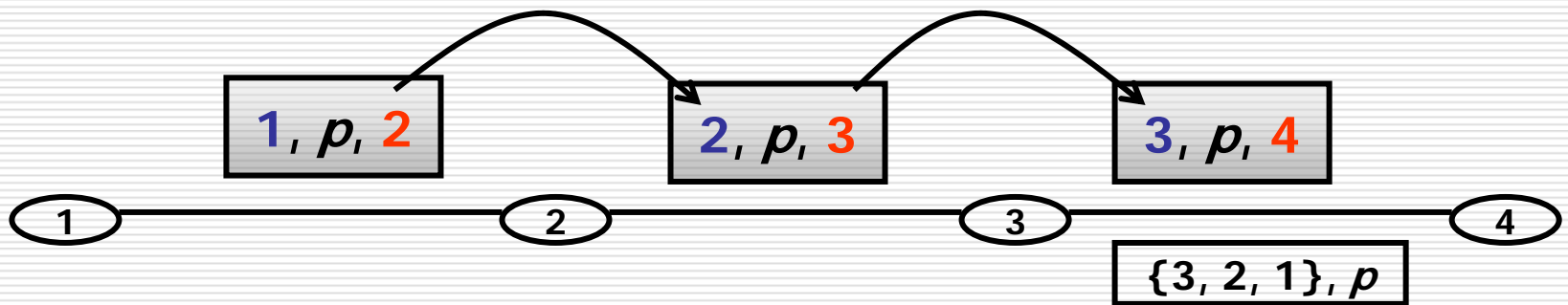
Address Attestations (AAs)

- IP address owners create AAs
 - X.509 Certificates for IP address allocation
 - $(\text{prefix}_1, \dots, \text{prefix}_k, \text{org}_y)$ address assignment
 - Routers create RAs
 - X.509 Certificates for AS# and Routers
 - $(\text{AS}, \text{AS}\#, \text{PK})$ binding
 - $(\text{RtrID}, \text{AS}\#, \text{PK})$ binding
-



S-BGP Route Attestations (RAs)

- ❑ Router signs (new AS number, prefix, next_hop)
- ❑ Sends all previous signatures
- ❑ Verify aspath {1, 2, 3}
 - Needs 3 signatures
- ❑ Sign aspath {1, 2, 3}
 - Creates n signatures

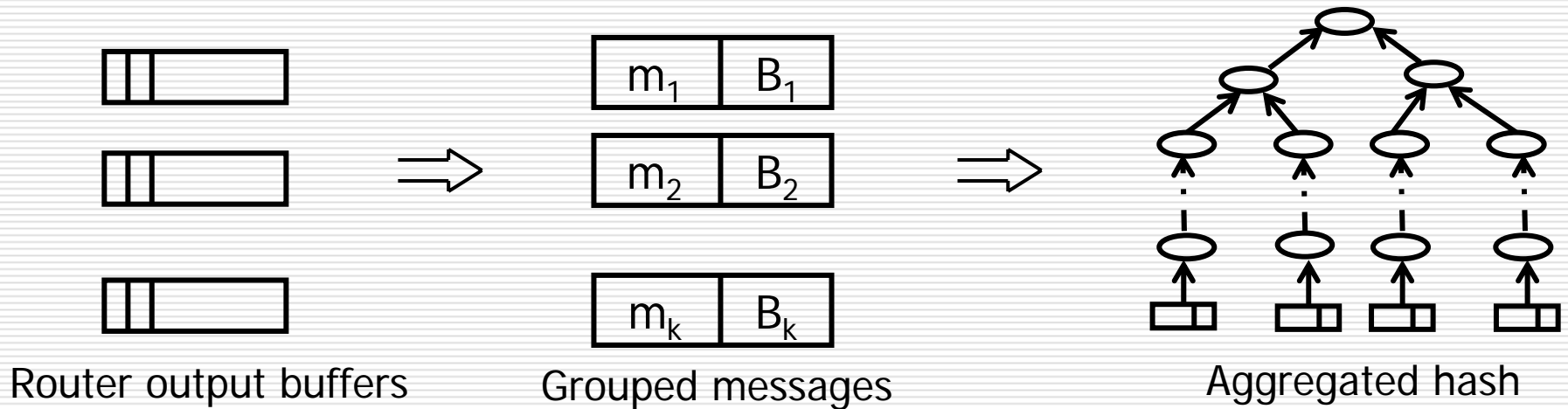


- ❑ Signature Algorithm—DSA



Signature Amortization (S-A)

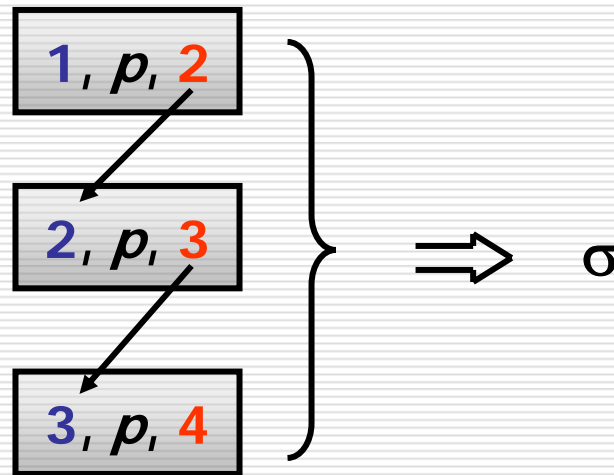
- Fast signature verification—RSA
- Few signature signing—aggregate messages
 - Bit vectors
 - Merkle hash trees
- Auxiliary values for each signature





Sequential Aggregate Signature

- k signers $\{s_1, s_2, \dots, s_k\}$
 k messages $\{m_1, m_2, \dots, m_k\}$
 \Rightarrow one aggregate signature σ

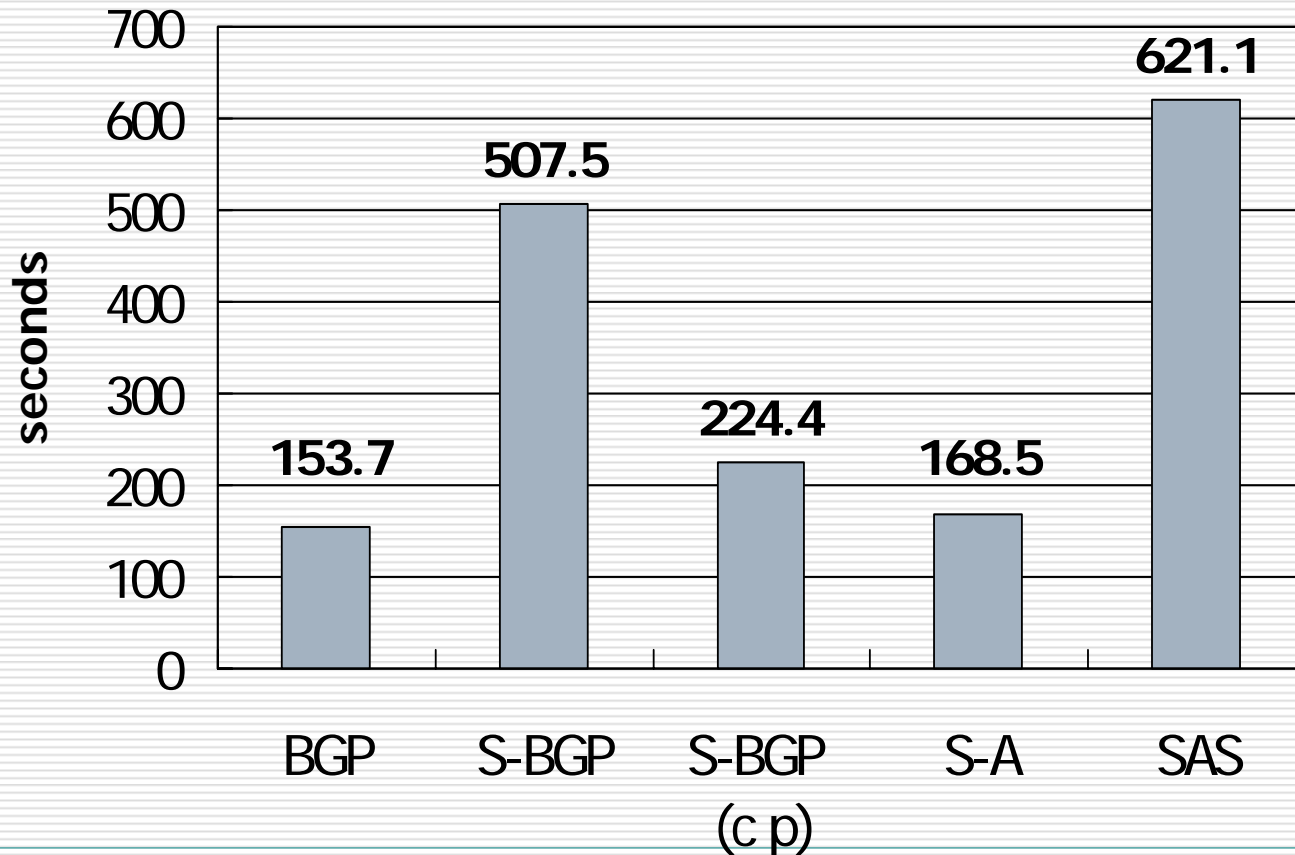


- One aggregate signature for entire AS path



PA Signature Performance—Convergence

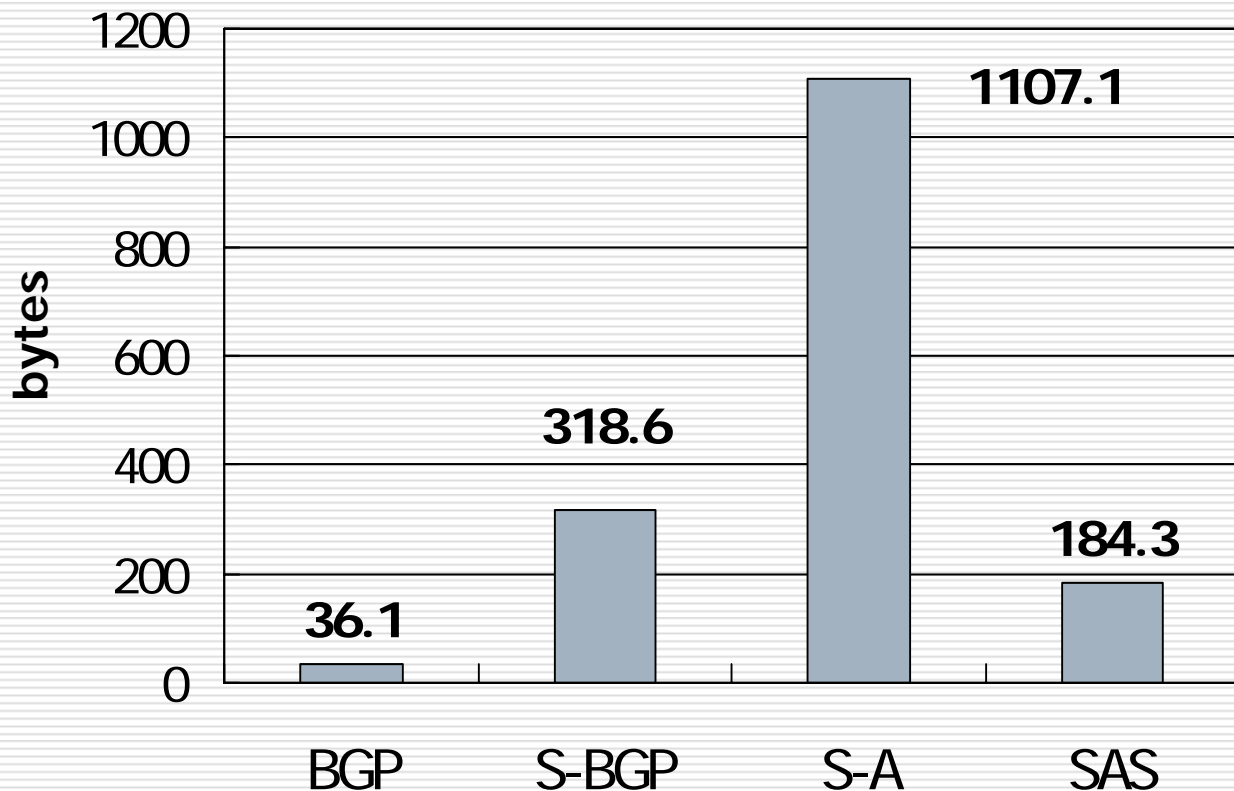
- *S-A converges fast* — aggregates 60 messages





PA Signature Performance—Message

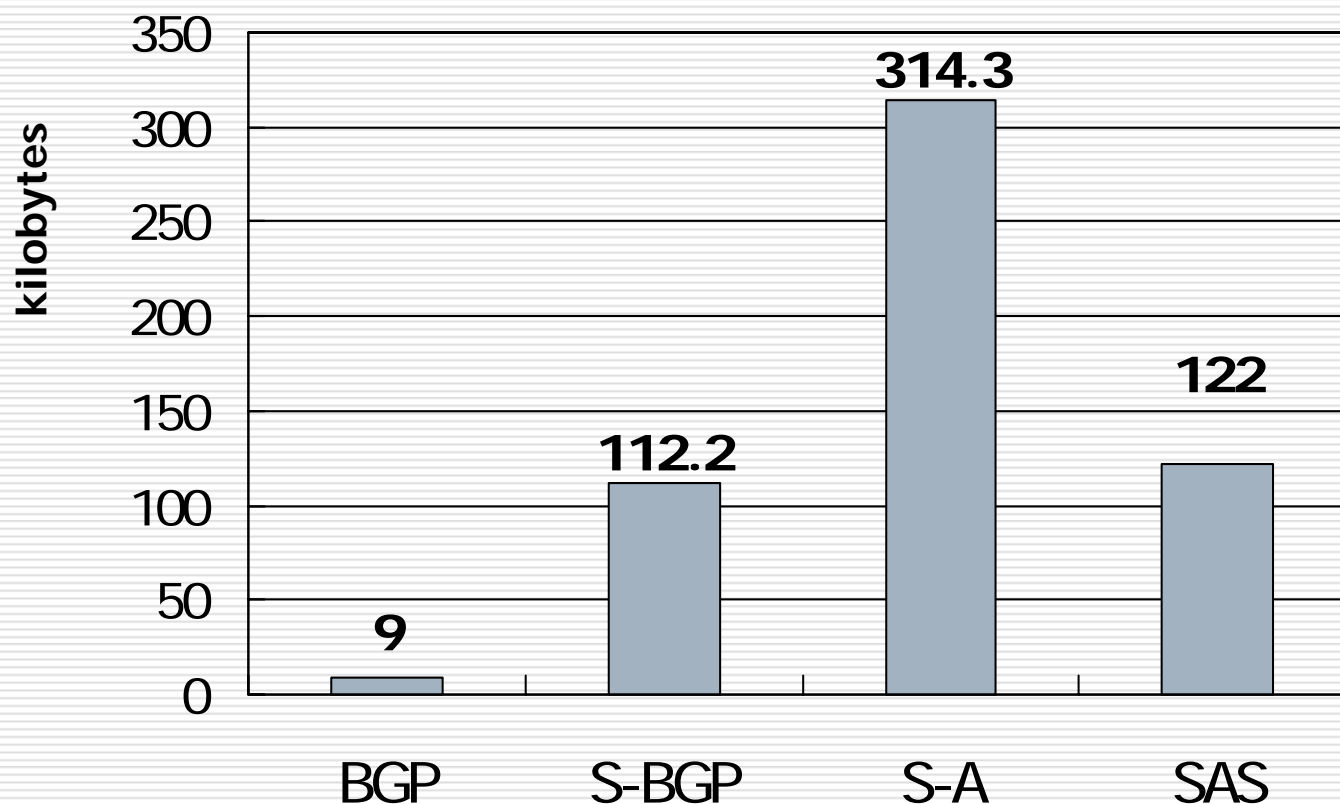
- SAS — shortest messages
- S-A — longest messages





PA Signature Performance—Memory

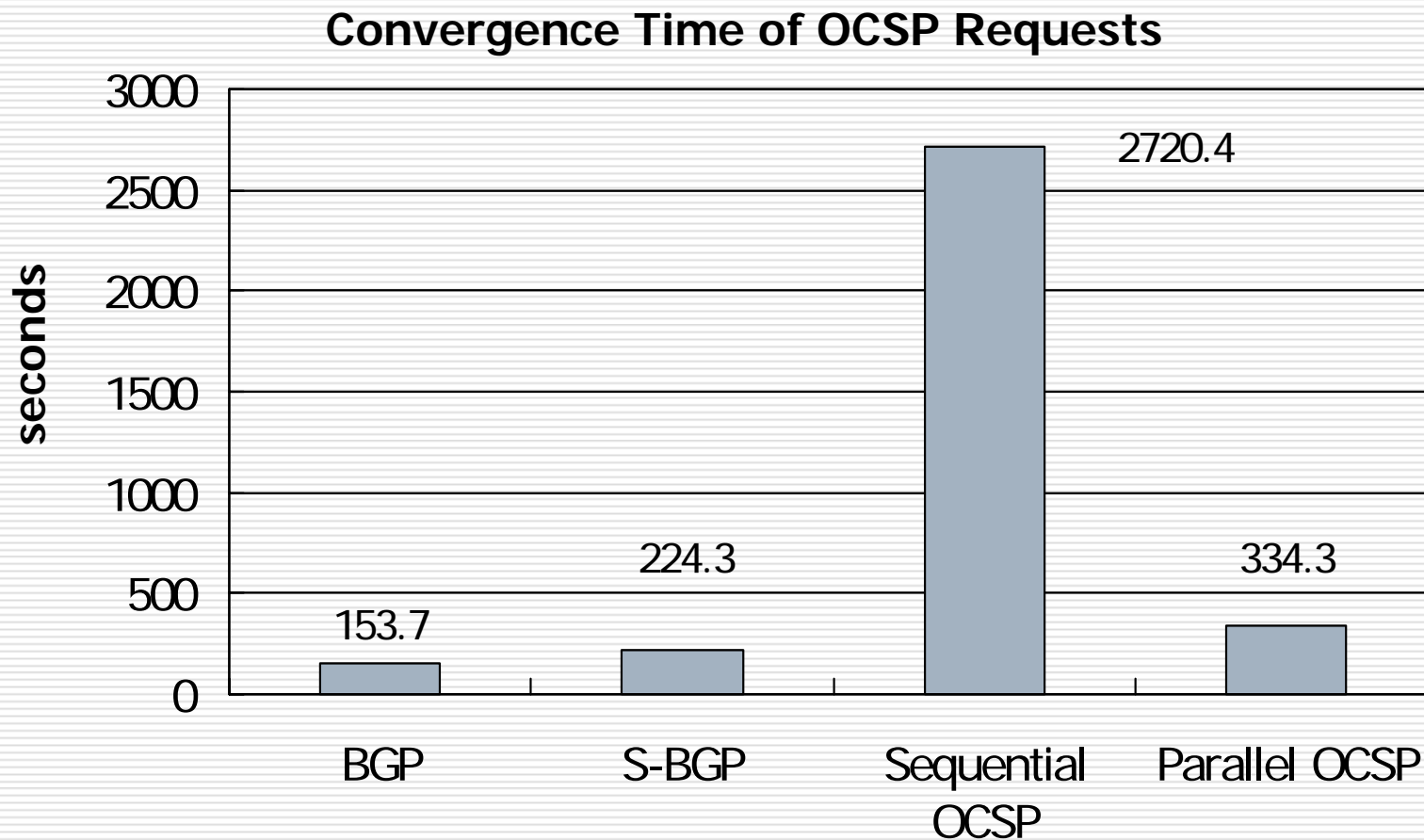
□ S-A — expensive on memory





PA PKI Performance—OCSP Requests

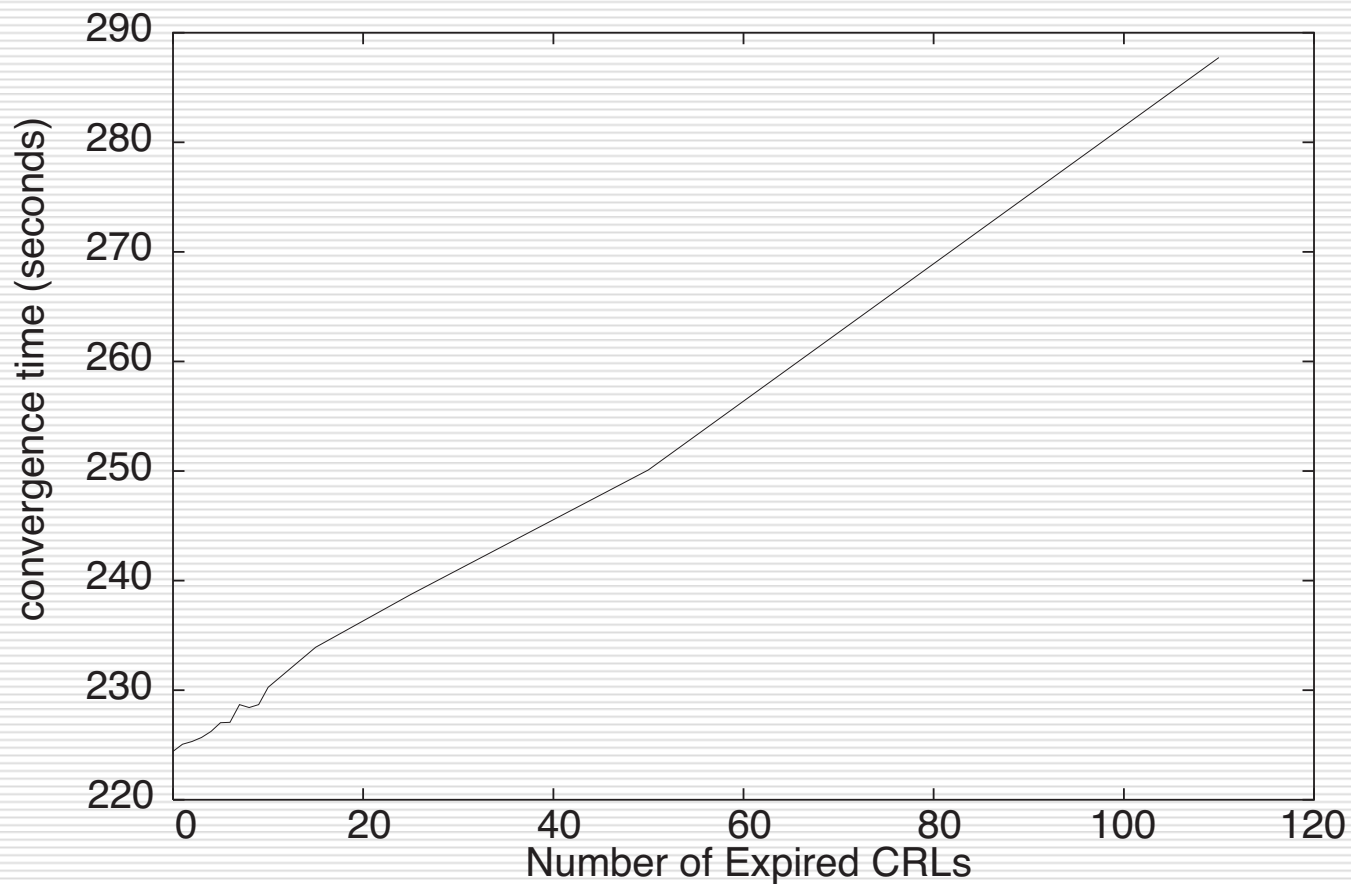
□ \approx 88,000 OCSP requests





PA PKI Performance—CRLs Fetching

Convergence Time of CRL fetching





Related Work

- S-BGP [Kent:NDSS00]
 - OASim [Aiello:CCS03]
 - psBGP [Wan:NDSS05]
 - Listen and Whisper [Subramanian:NSDI04]
 - Symmetric cryptography
 - Potentially more efficient
 - Key distribution [Goodrich00]
 - Time synchronization [Hu:SIGCOMM04]
-



Conclusions

- PKI proposed for a REAL problem
 - Large-scale network simulation
 - Performance trade-offs
 - PKIs
 - S-BGP cert out-of-band transmission *vs.* OA in-band transmission
 - OCSP timely notification *vs.* CRLs fast status checking
 - Signature processing
 - S-A fast speed *vs.* SAS short messages
-



Next Steps

- More efficient public key cryptography
 - Combine S-A and SAS
 - Certificate-using decisions
 - Revoke routes, if a certificate is revoked?
 - Comprehensive PKI simulation model
 - Issuing/revoking activity
 - Certification path discovery/validation
-



Thank you!

- Sun Microsystems
 - Mellon Foundation
 - Cisco Systems
 - Intel Corporation
 - NSF
 - DoJ/DHS

 - Email zhaom@cs.dartmouth.edu
 - Homepage <http://www.cs.dartmouth.edu/~zhaom>
-



Benchmarks

	SHA-1 hash	MD5 hash	Attestations	Certificates	Identifier
Length	20 bytes	16 bytes	110 bytes	600 bytes	4 bytes

	RSA	DSA	DSA(p)	SAS
Verify Time (ms)	2.5	31.0	31.0	2.5
Sign Time (ms)	50.0	25.5	0.015	50.0
Signature length (bytes)	128	40	40	128

	OCSP request	CRL fetching
Operation latency (second)	0.5—1.0	0.5—1.0
