BGPSEC : A BGP Extension to Support AS-Path Validation

Matt Lepinski

BBN Technologies

What is BGPSEC?

- Proposal for securing the AS-PATH attribute
- Extension to BGP that is negotiated as a new capability (RFC 5492)
- An optional path attribute that contains a list of cryptographic signatures that protect the AS-PATH

Goals and Non-Goals

- Goal: To ensure the integrity of the NRLI and AS-PATH attribute in a BGP Update

  Example: an update X.Y/16 with AS-PATH: AS 1, AS 2, AS 3

  Upon Receipt of this update, AS 4 is assured that
  - AS 1 originated a route for X.Y/16 and sent it to AS 2
  - AS 2 received this route from AS 1 and sent it to AS 3
  - AS 3 received this route from AS 2 and sent it to AS 4

- Non-Goal : Anything having to do with the data path!

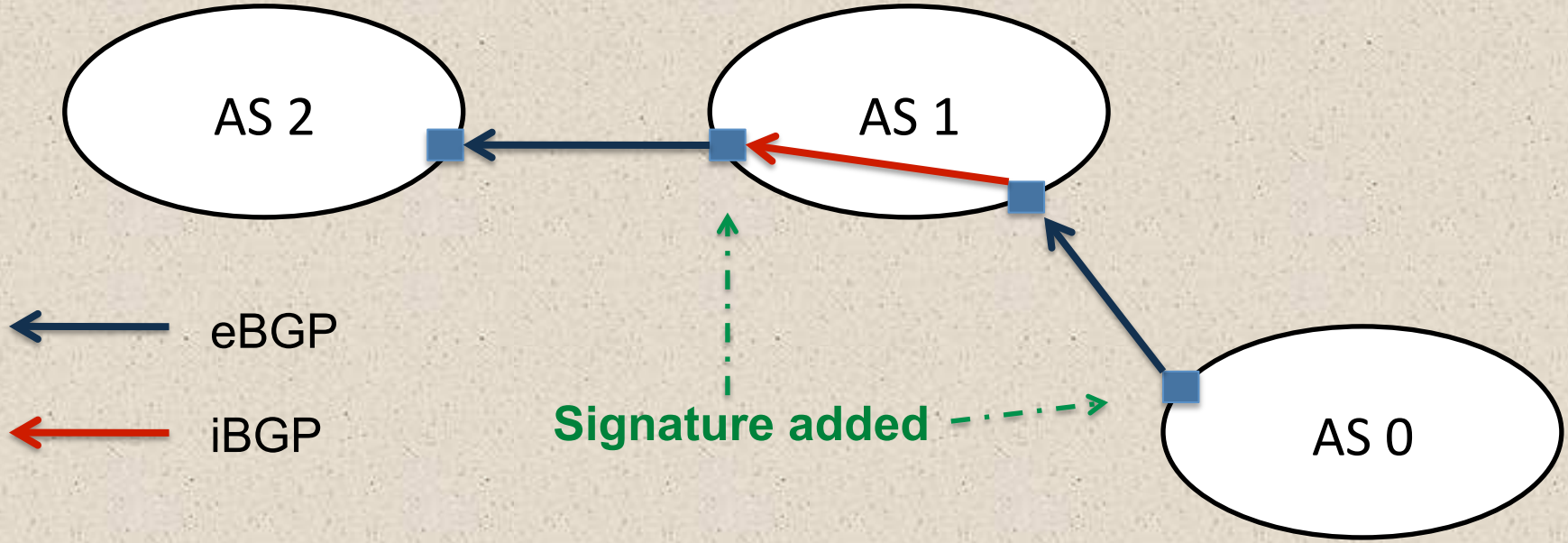
The -00 drafts

- Please read:
  - draft-lepinski-bgpsec-overview-00
  - draft-lepinski-bgpsec-protocol-00
- A first cut at specifying an incrementally deployable BGP extension for securing the AS-Path
  - Focus: simple, understandable protocol with correct semantics
  - No attempts whatsoever were made to optimize computation time, storage space, network traffic, etc
- For List Discussion: Do these documents describe an approach that the SIDR WG wants to pursue?

Negotiating BGPSEC

- BGPSEC only between consenting routers
- BGPSEC capability contains
  - Send bit == "I am willing to send the BGPSEC attribute"
  - Receive bit == "I am willing to receive the attribute"
  - AFI : IPv4 and IPv6 negotiated separately
- Adding signatures can make update messages big
  - In order to receive BGPSEC you probably need to support updates larger than 4096 bytes
  - See: draft-ymbk-bgp-extended-messages
- Note: Permit negotiation of simplex BGPSEC because sending is much easier than receiving

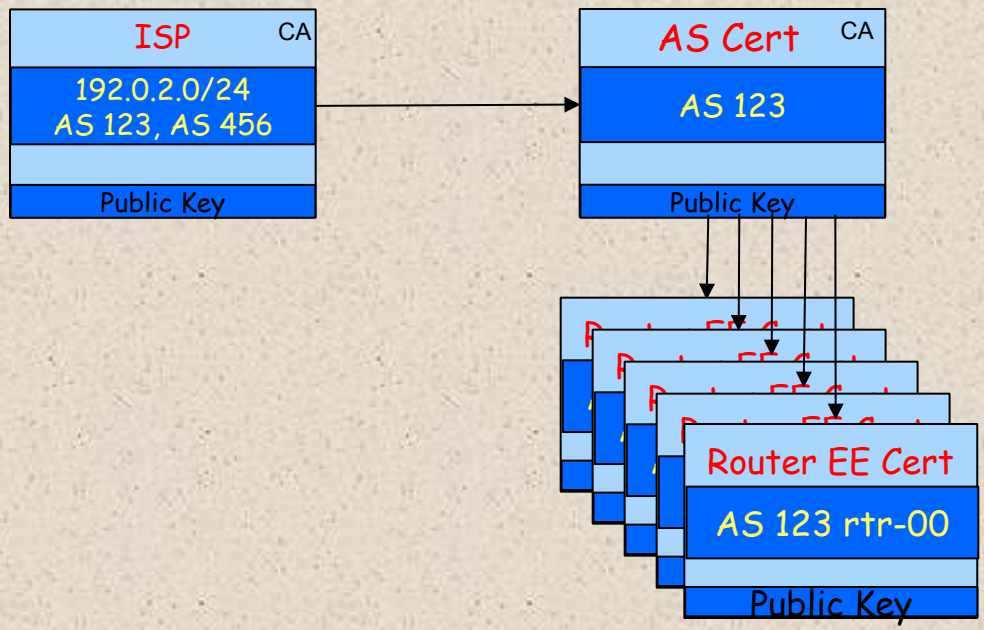
Signing at Provider Boundaries



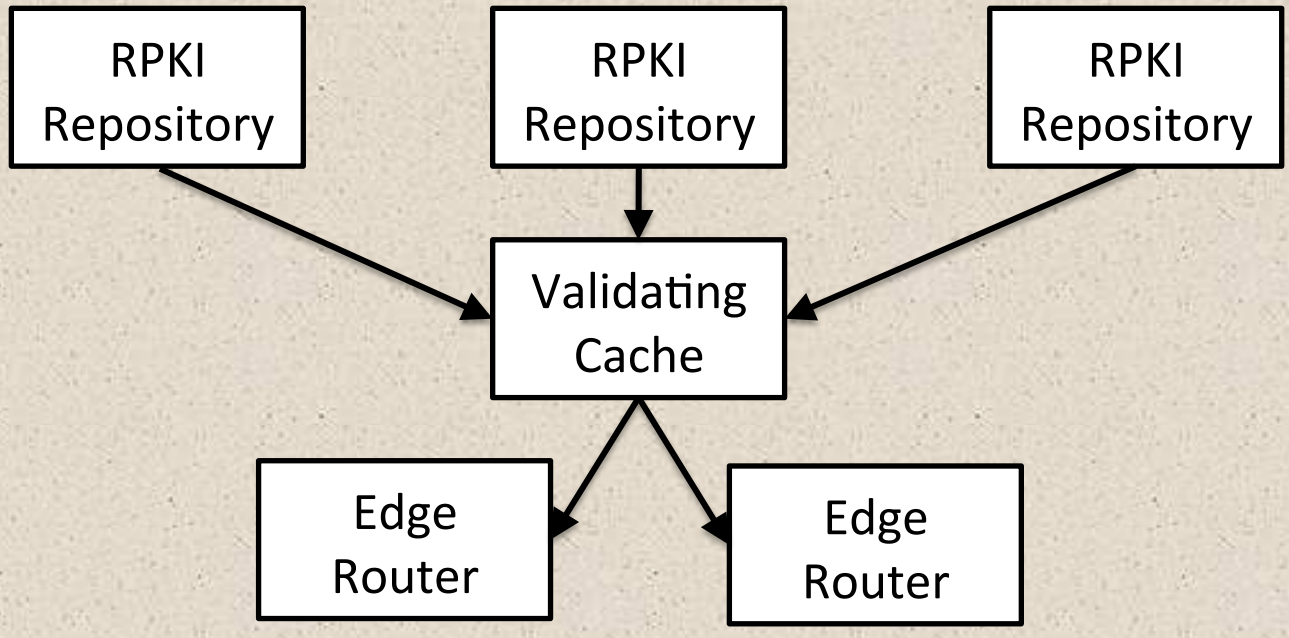
- Protects only interdomain routing, not iBGP
- Signatures are added when a route announcement leaves an AS
- However, iBGP needs to carry BGPSEC signatures

End-Entity Certificates for Routers

- Extend the RPKI to include new end-entity certs
  - Issued under the CA certificate for an AS
  - Private keys held by the AS's edge routers
  - Can do one key per router, or share common keys

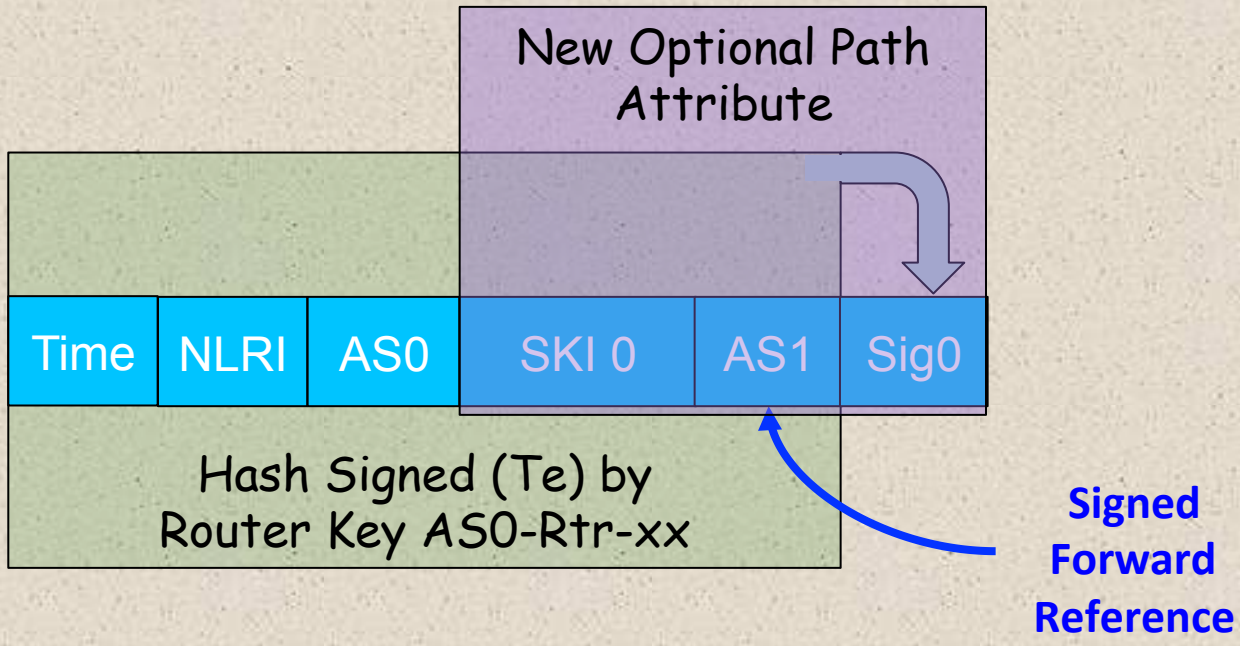


BGPSEC and the RPKI



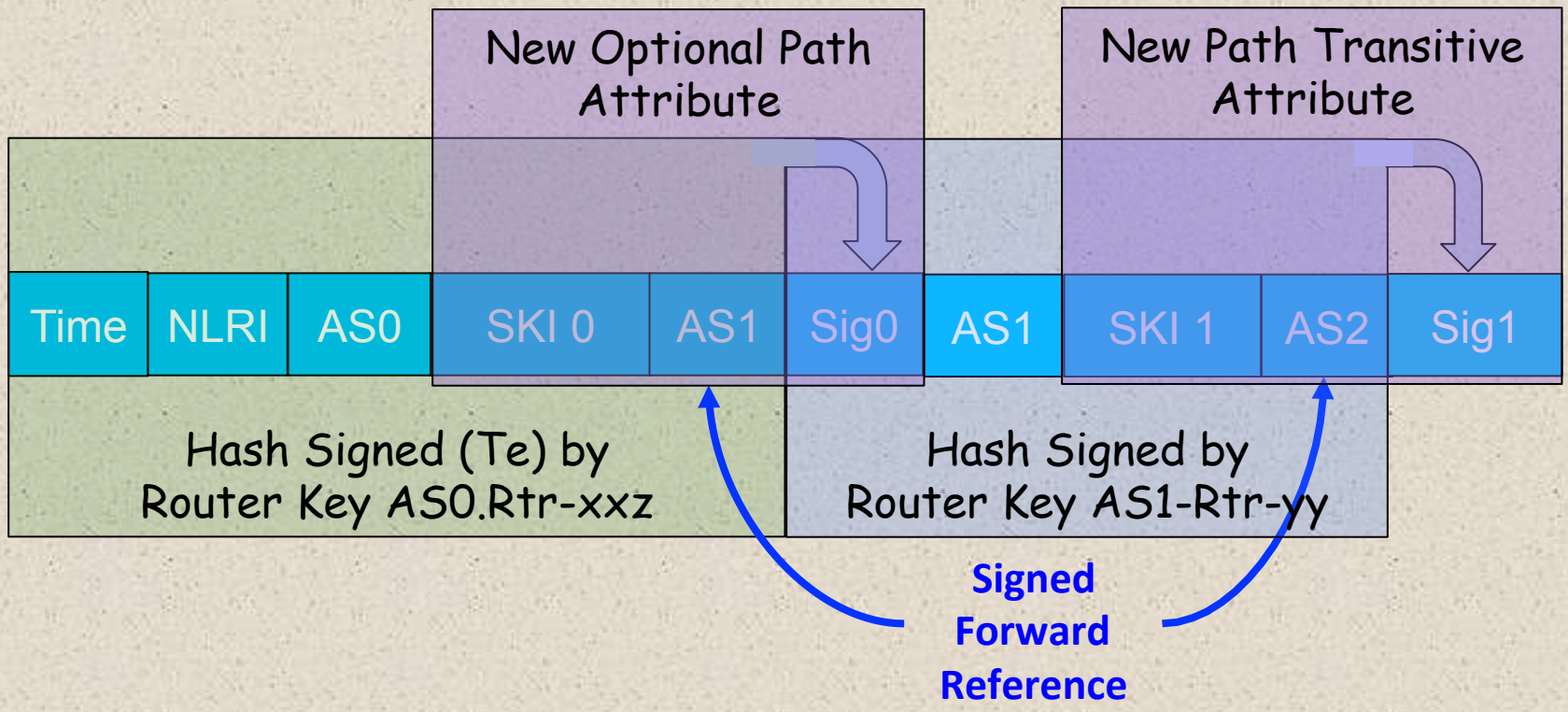
- To send BGPSEC, a router needs only its private key
- To validate BGPSEC, a router needs
  - (SKI, Public Key, AS) triples from valid certs
  - Origin validation data

What Data is Signed (1/2)



- The Signature of AS 0 includes the AS number of the peer to whom the update is being sent
- The SKI is used by the recipient to look-up the public key needed to verify the signature

What Data is Signed (2/2)



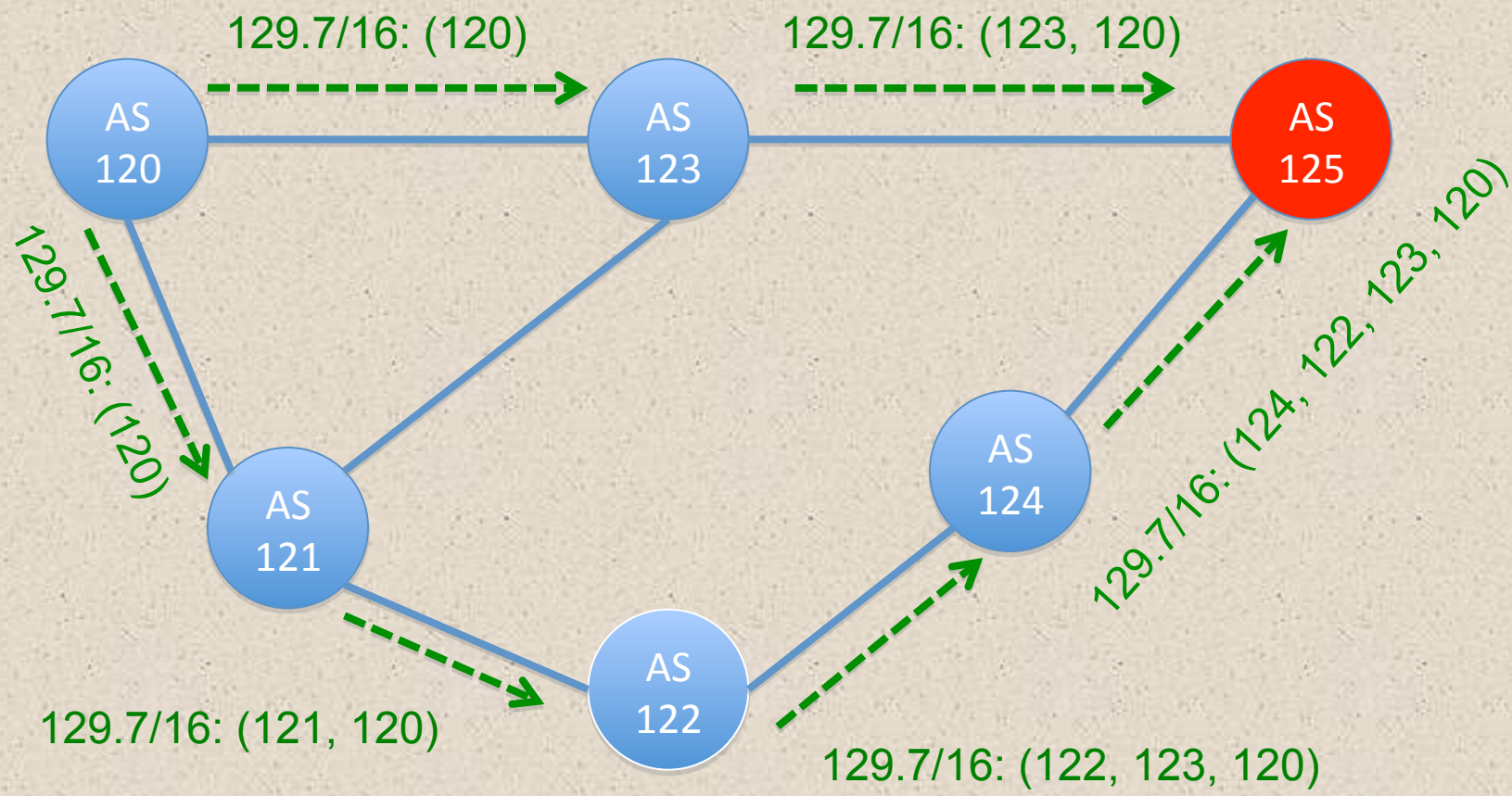
- The signature of AS 1 covers the signature of AS 0 plus new fields added by AS 1
- When AS 2 receives the update message it contains signatures from both AS 1 and AS 0

To see such signatures are useful …

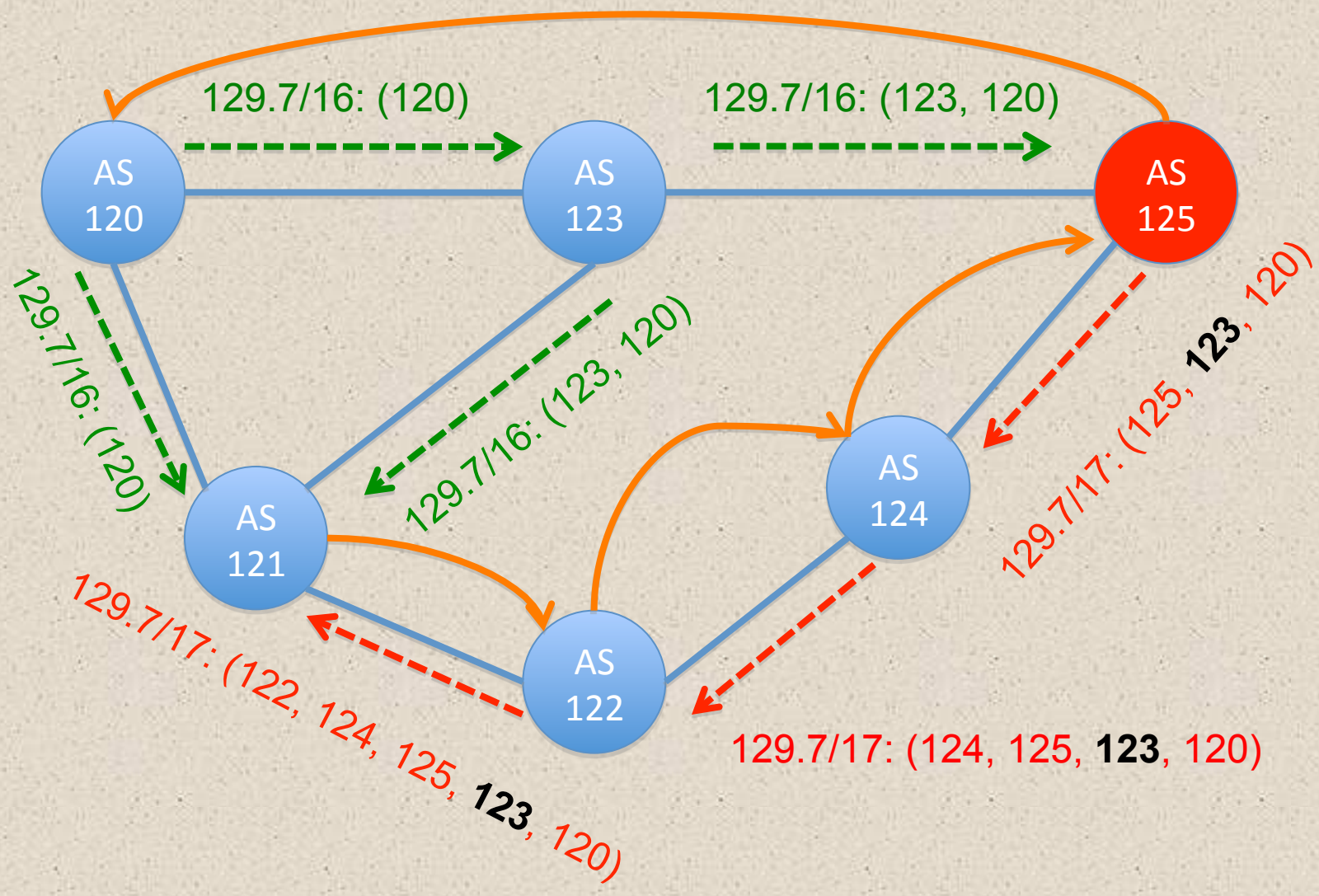
… recall the threats presentation

Kapela/Pilosov Attack (1/2)

AS 125 wants to be a MITM for traffic to 129.7/16



Kapela/Pilosov Attack (2/2)



Note on Signing the NLRI

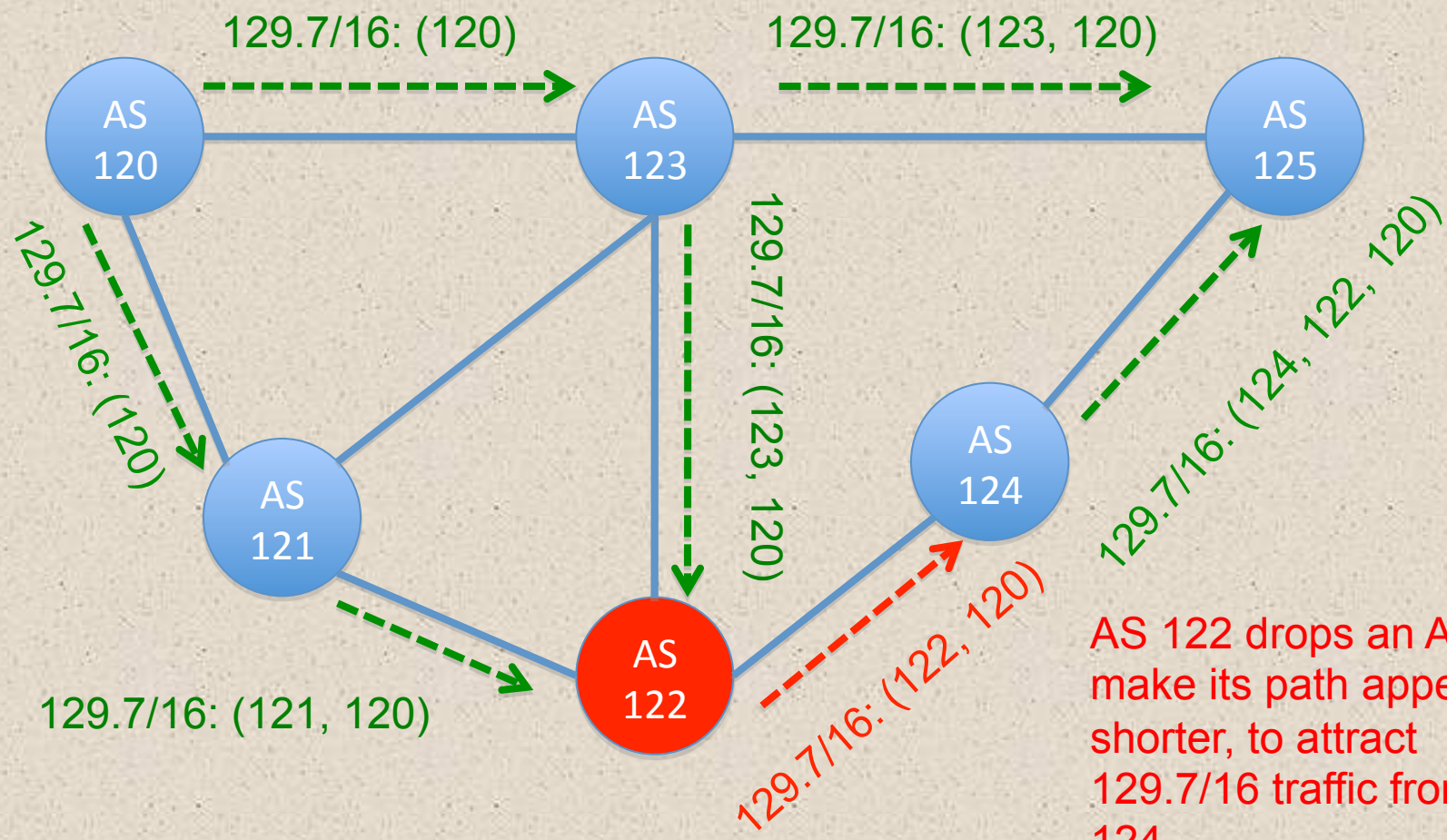
- The signature of the origin AS covers the NLRI in the update
- Therefore, changing the NLRI breaks the signature
- This is important so an adversary does not change a received prefix (e.g., lengthen it)
- BGPSEC does not currently support multiple prefixes in the NLRI of a single update
  - To avoid problems if a later AS only advertised one of a set of received prefixes
- Possible area to explore future optimizations

But changing the NLRI is not the only way to attract traffic …

Dropping an AS

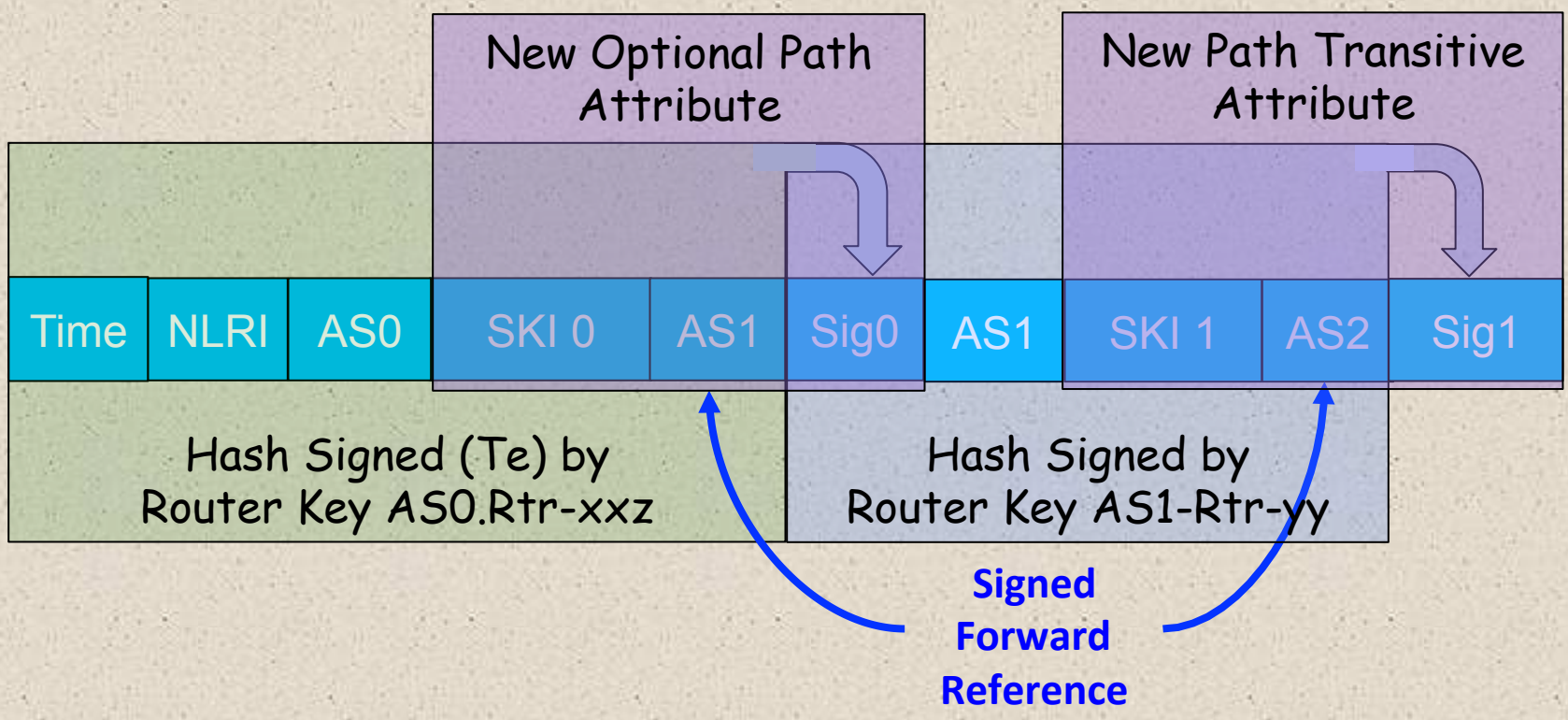
AS 120 has a ROA for 129.7/16

AS 122 wants to be a MITM for traffic to 129.7/16

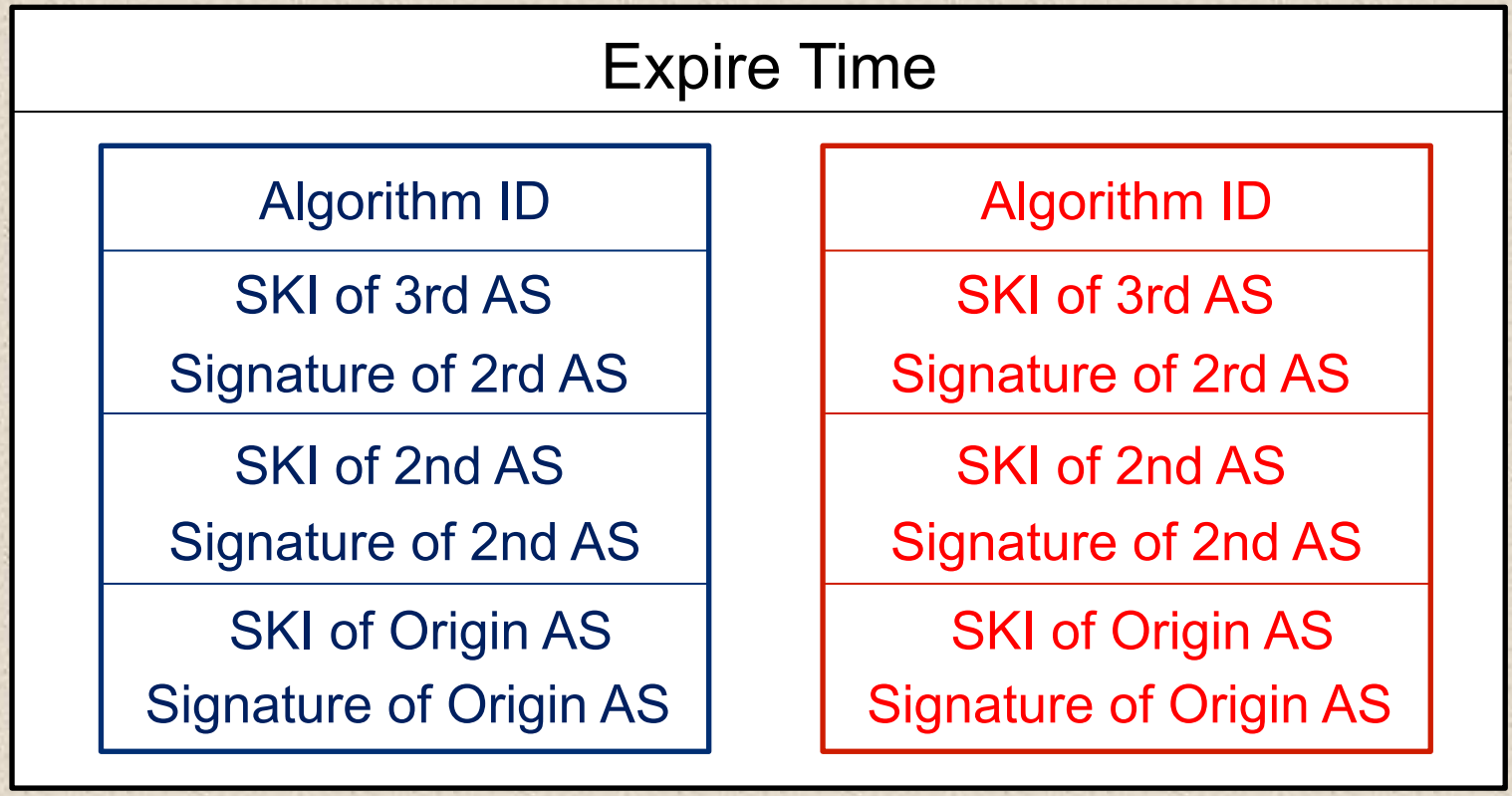


AS 122 drops an AS to make its path appear shorter, to attract 129.7/16 traffic from AS 124

What Data is Signed



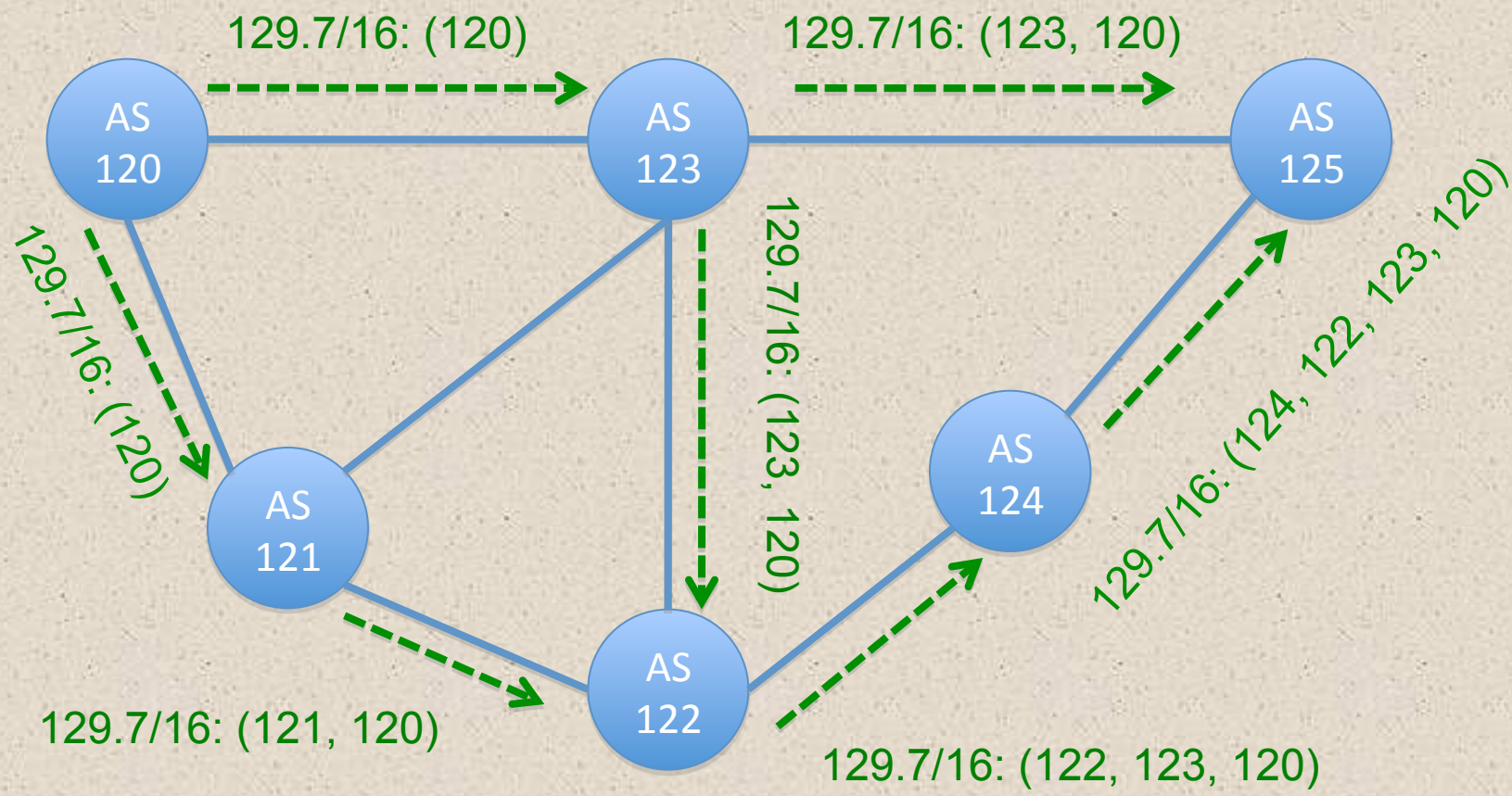
BGPSEC_Path_Signatures Attribute



- Note: Red block of signatures is optional and is used only to facilitate algorithm transition
- Expire Time? … let's recall the threats presentation …

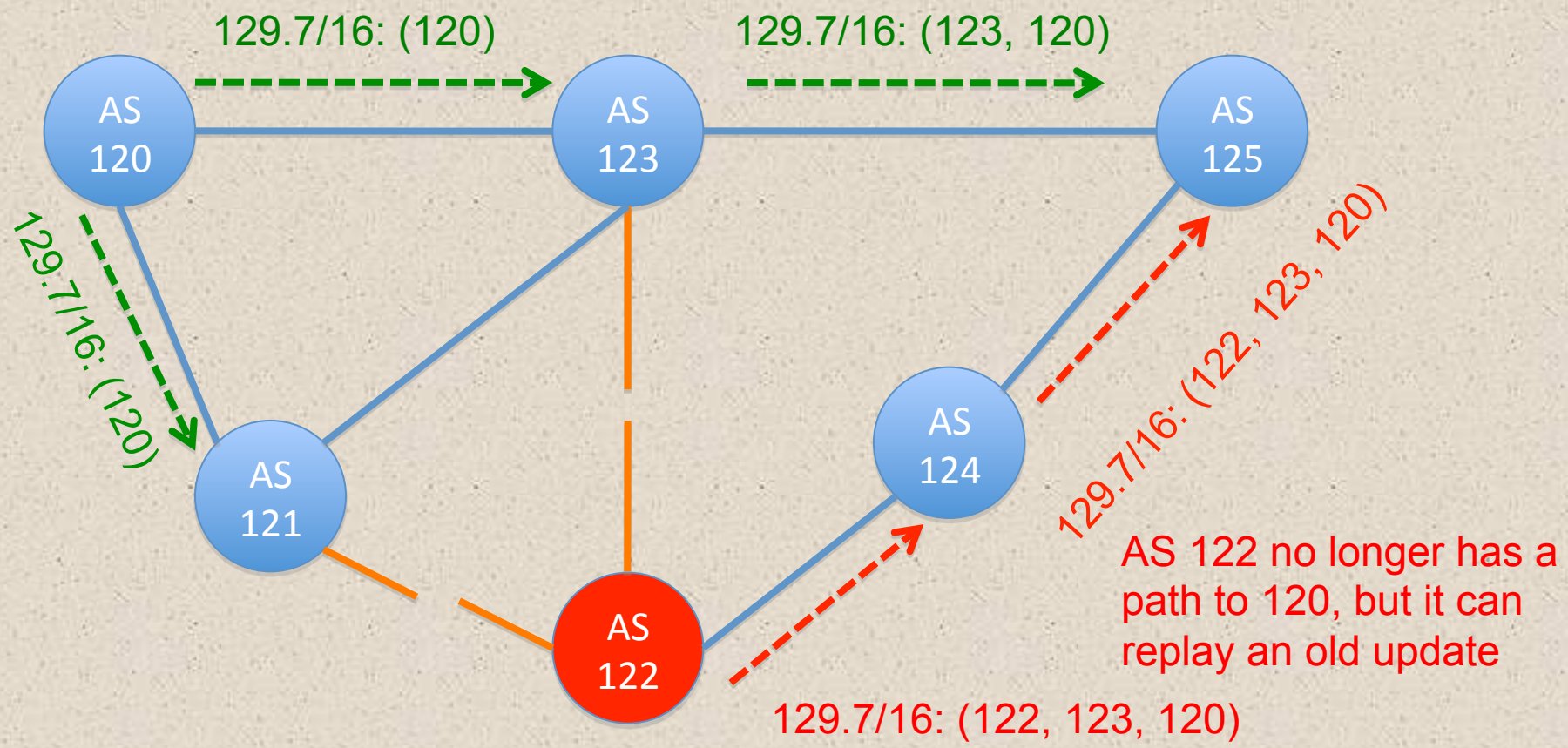
Hijack via Update Replay (1/2)

AS 120 has a
ROA for 129.7/16



Hijack via Update Replay (2/2)

AS 120 has a
ROA for 129.7/16



Expire Time and Beaconing

- Origin of a route announcement selects the Expire Time
- Expire Time limits the window of vulnerability to replay attacks
- New prefix announcement needs to be made well before the Expire Time is reached, AKA ***beaconing***
- Natural trade-off:
  - Short expire time means stronger replay protection
  - Longer expire time means less BGP traffic

BGPSEC Validation

- Recipient validates as follows:
  - Check the expire time
  - Perform origin validation
  - Fetch public keys and verify the AS in AS-PATH matches the AS from the router end-entity certificate
  - Verify the signatures <=== Crypto
- Validation need only be done upon receiving a signed update from external peer
- What you do with the validation state is completely up to your local policy!!

Final Notes

- Incrementally deployable
  - An AS can use BGPSEC for only some prefixes or only at certain edge routers
- Protects only the AS-PATH attribute and the NLRI
  - Consistent with the current SIDR charter
  - Consistent with our current understanding of threats and desired BGP semantics
- Cryptographic algorithm agility
  - Specification outlines a procedure for changing algorithms
  - As with the RPKI, algorithm transitions are expensive and global

Co-Authors

- Rob Austein, ISC
- Steven Bellovin, Columbia Univ
- Rany Bush, IIJ
- Russ Housley, Vigilsec
- Stephen Kent, BBN
- Warren Kumari, Google
- Doug Montgomery, NIST
- Kotikalapudi Sriram, NIST
- Samuel Weiler, Sparta

Valuable Review and Contribution

- Luke Berndt
- Sharon Goldberg
- Ed Kern
- Chris Marrow
- Doug Maughan
- Pradosh Mohapatra
- Russ Mundy
- Sandy Murphy
- Keyur Patel
- Mark Reynolds
- Heather Schiller
- Jason Schiller
- John Scudder
- David Ward
- Ruediger Volk
- **Your Name Here!**