BGP Security in Partial Deployment Is the Juice Worth the Squeeze?

Robert Lychev
Georgia Tech
Boston University

Sharon Goldberg
Boston University

Michael Schapira
Hebrew University

General Theme

- Many widely used communication protocols on the Internet were not originally designed with security considerations in mind
- When working on designing and deploying new secure protocols we are faced with the following question:
  - How can we provide sufficient protection against attackers, while minimizing our resources and without introducing new complications?
- This is especially crucial, when the new secure protocols have to be partially deployed together with legacy insecure protocols

Partial Landscape of BGP Defenses

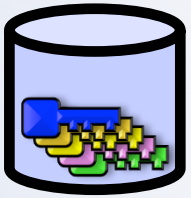
What does (partially-deployed) BGPSEC offer over RPKI?
(Or, is the juice worth the squeeze?)

- road to BGPSEC full-deployment is very tricky because introducing security only partially introduces new vulnerabilities
- not fully deployed BGPSEC provides only meager benefits over RPKI if network operators do not prioritize security in their routing policies

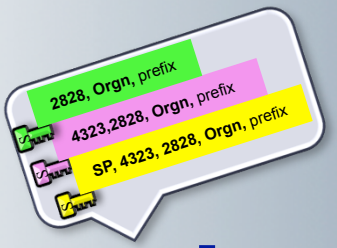
Security Benefits or Juice

- In deployment
- Crypto done offline

- In standardization
- Crypto done online



BGP and BGPSEC coexistence



BGP

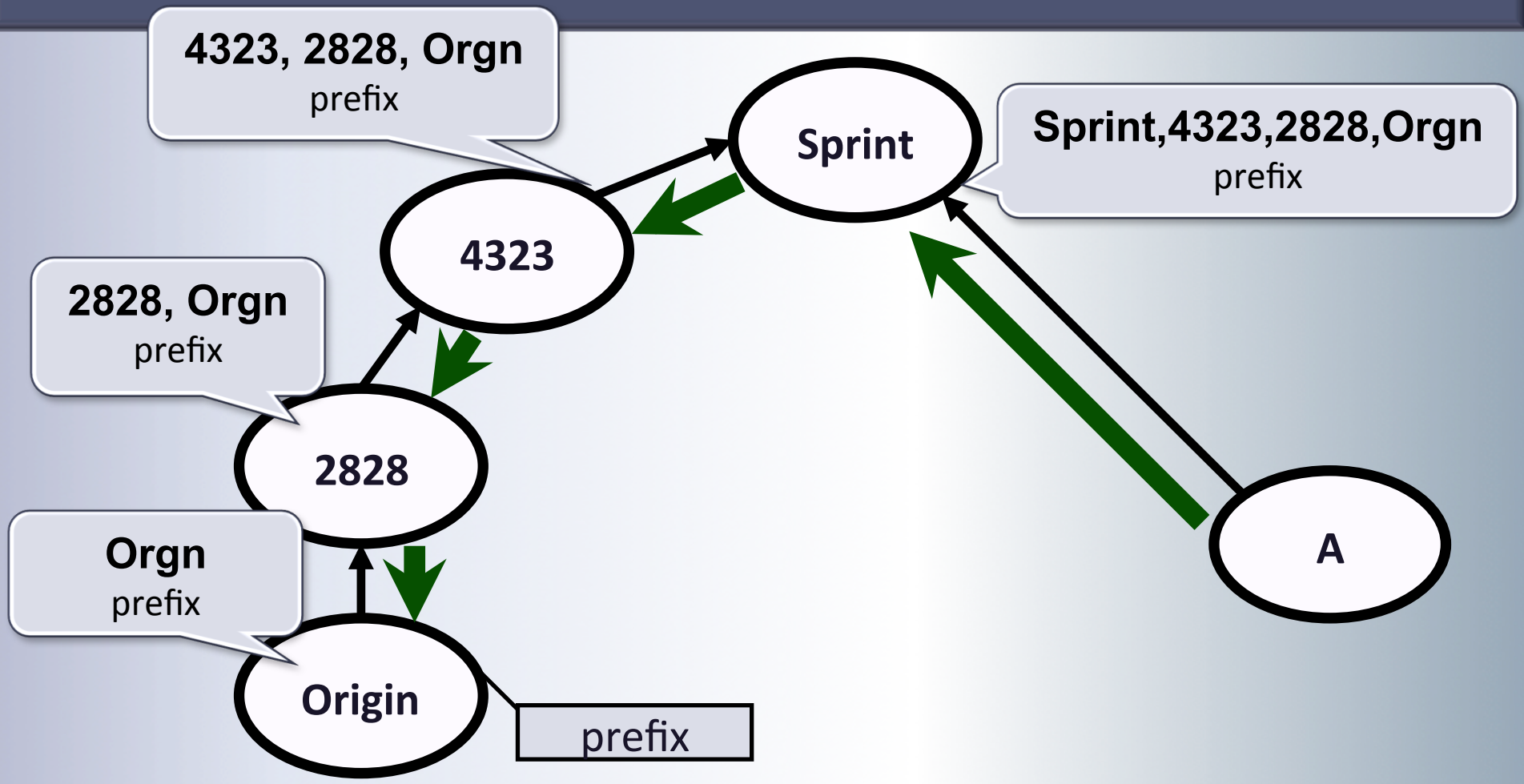
RPKI
(origin authentication)

BGPSEC

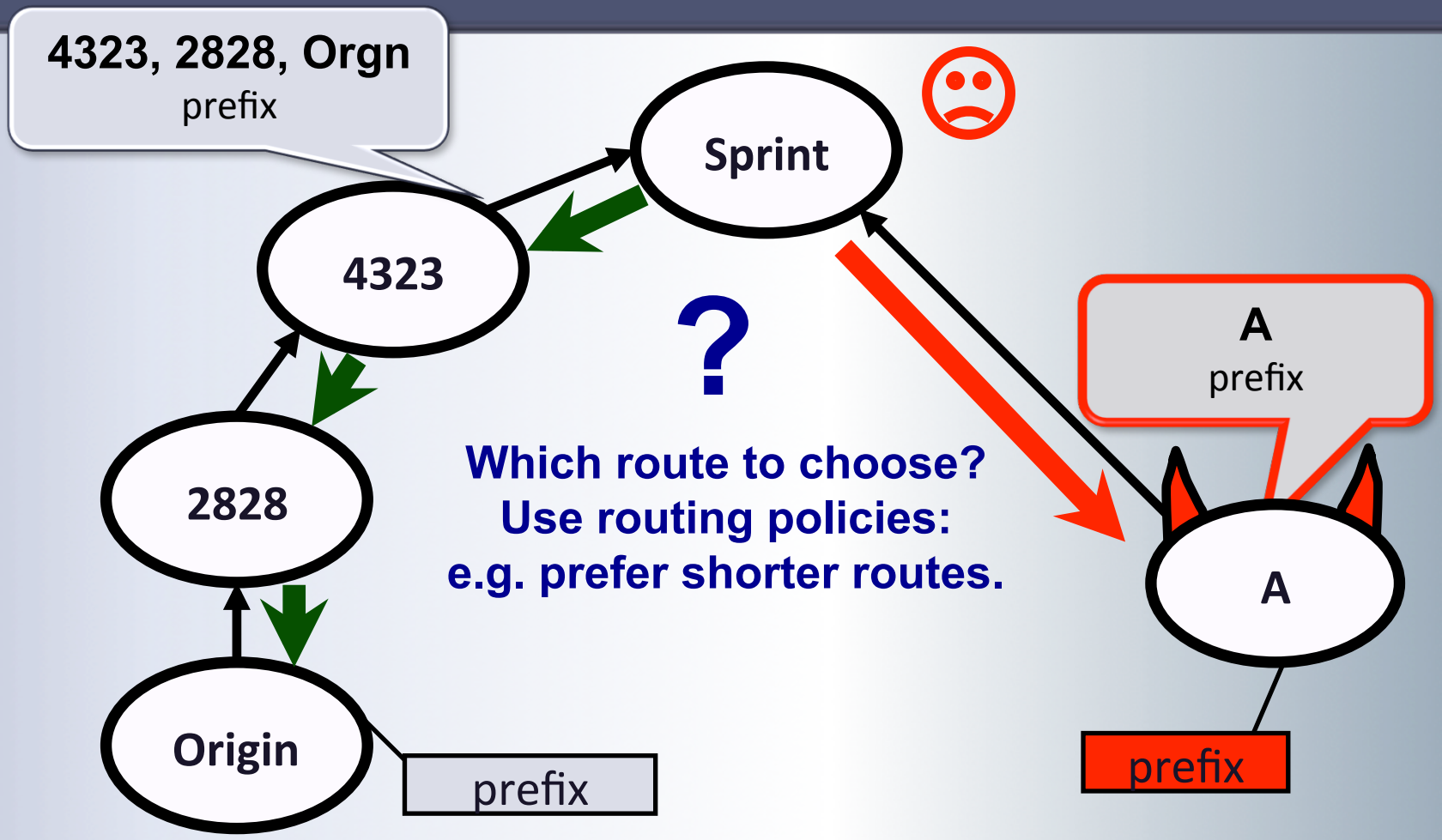
Outline

1. **Background:**
   1. BGP, RPKI, BGPSEC
   2. routing policies when BGPSEC is only partially deployed
2. BGPSEC in partial deployment is tricky
3. Is the juice worth the squeeze?
4. Summary

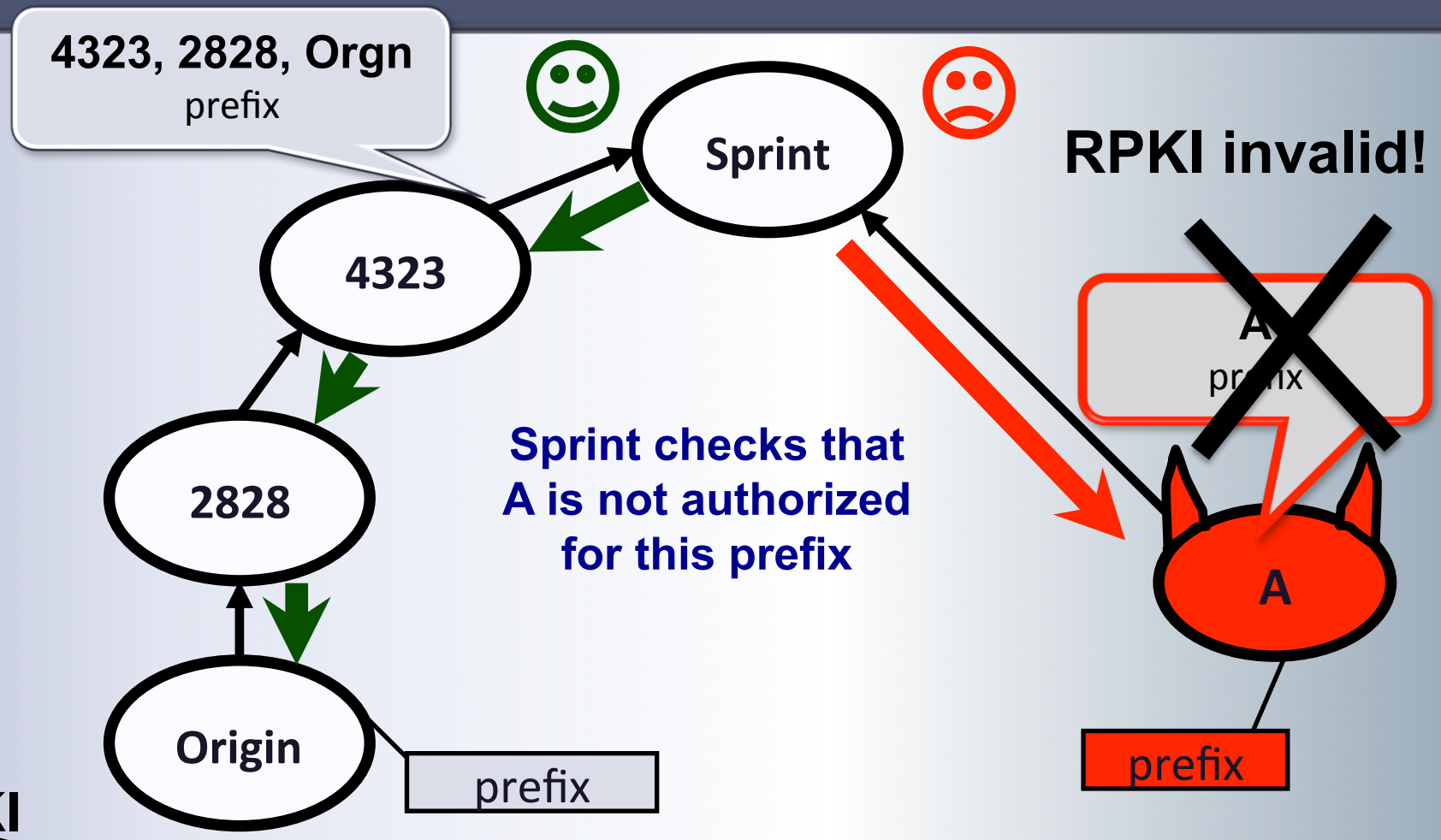
The Border Gateway Protocol (BGP)



Prefix Hijack

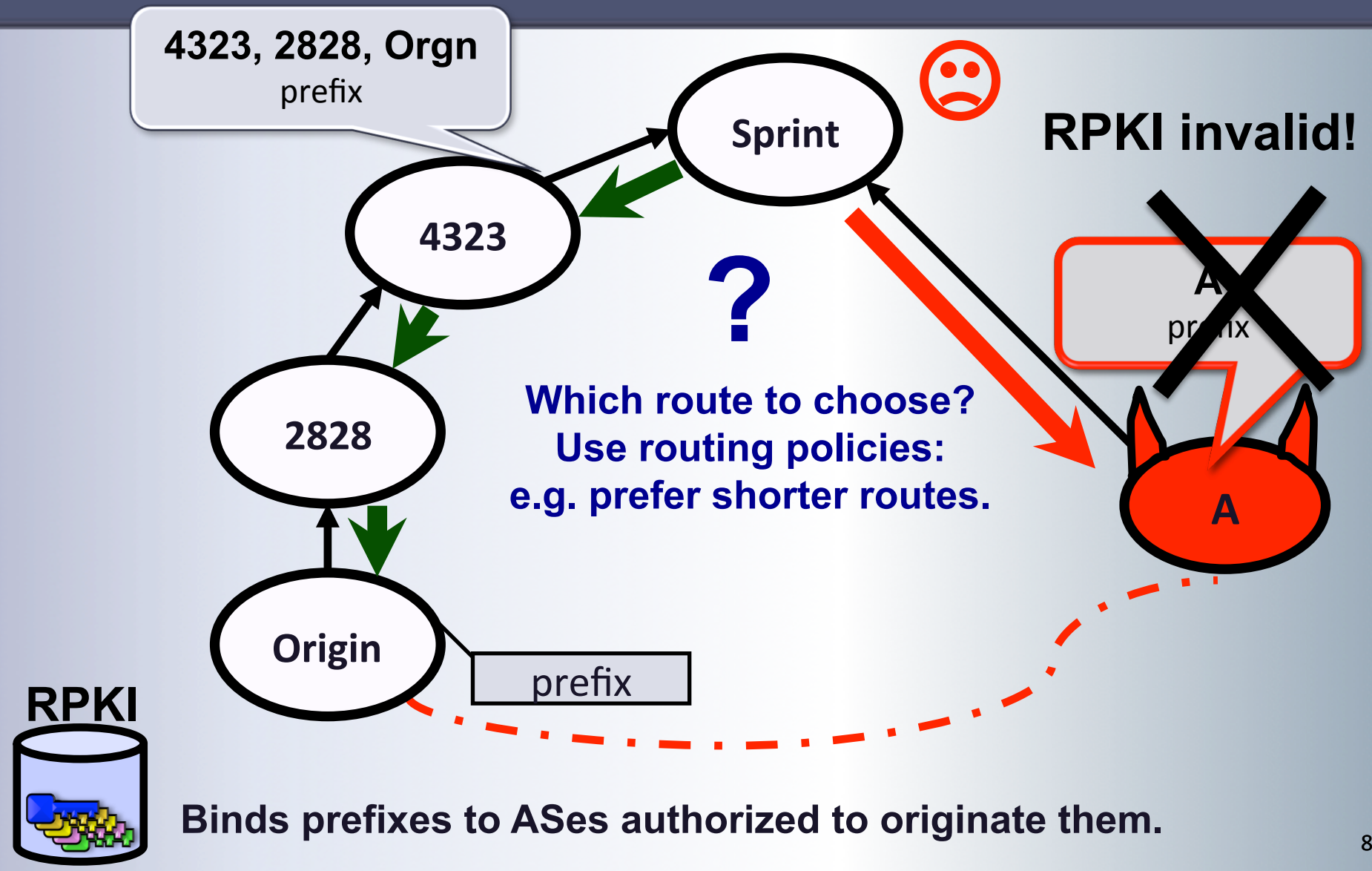


RPKI Prevents Prefix Hijacks



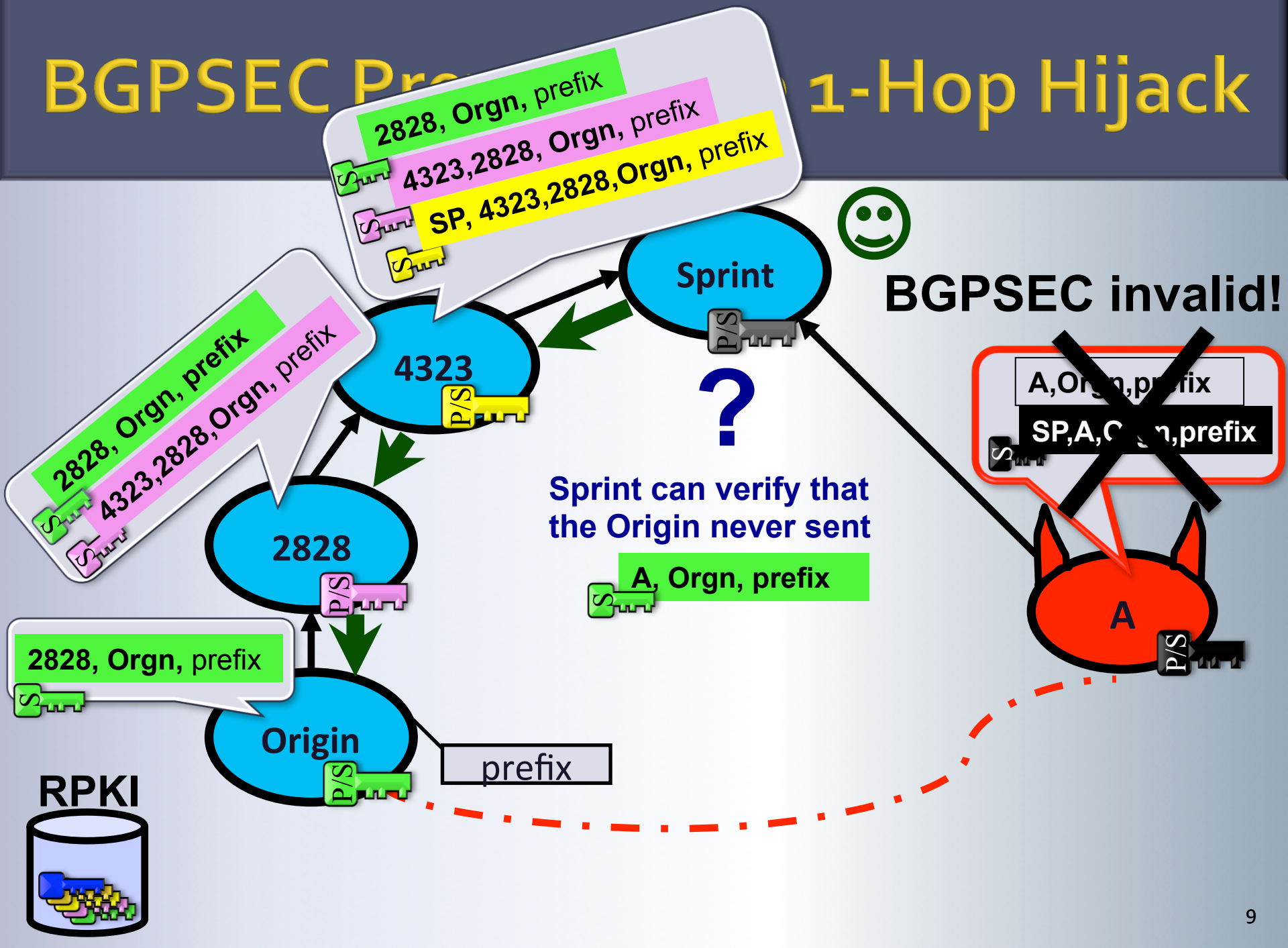
Binds prefixes to ASes authorized to originate them.

The 1-Hop Hijack

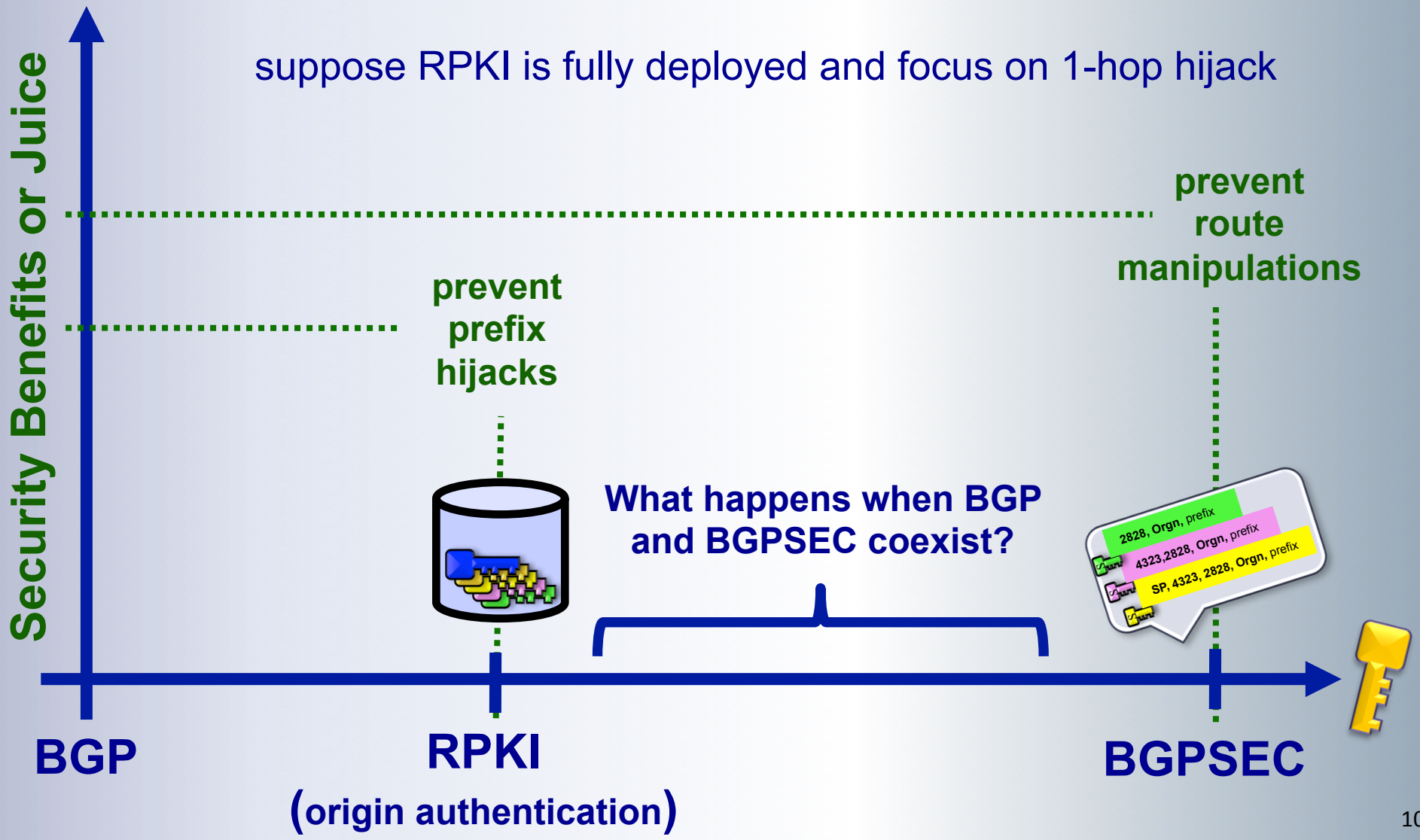


Binds prefixes to ASes authorized to originate them.

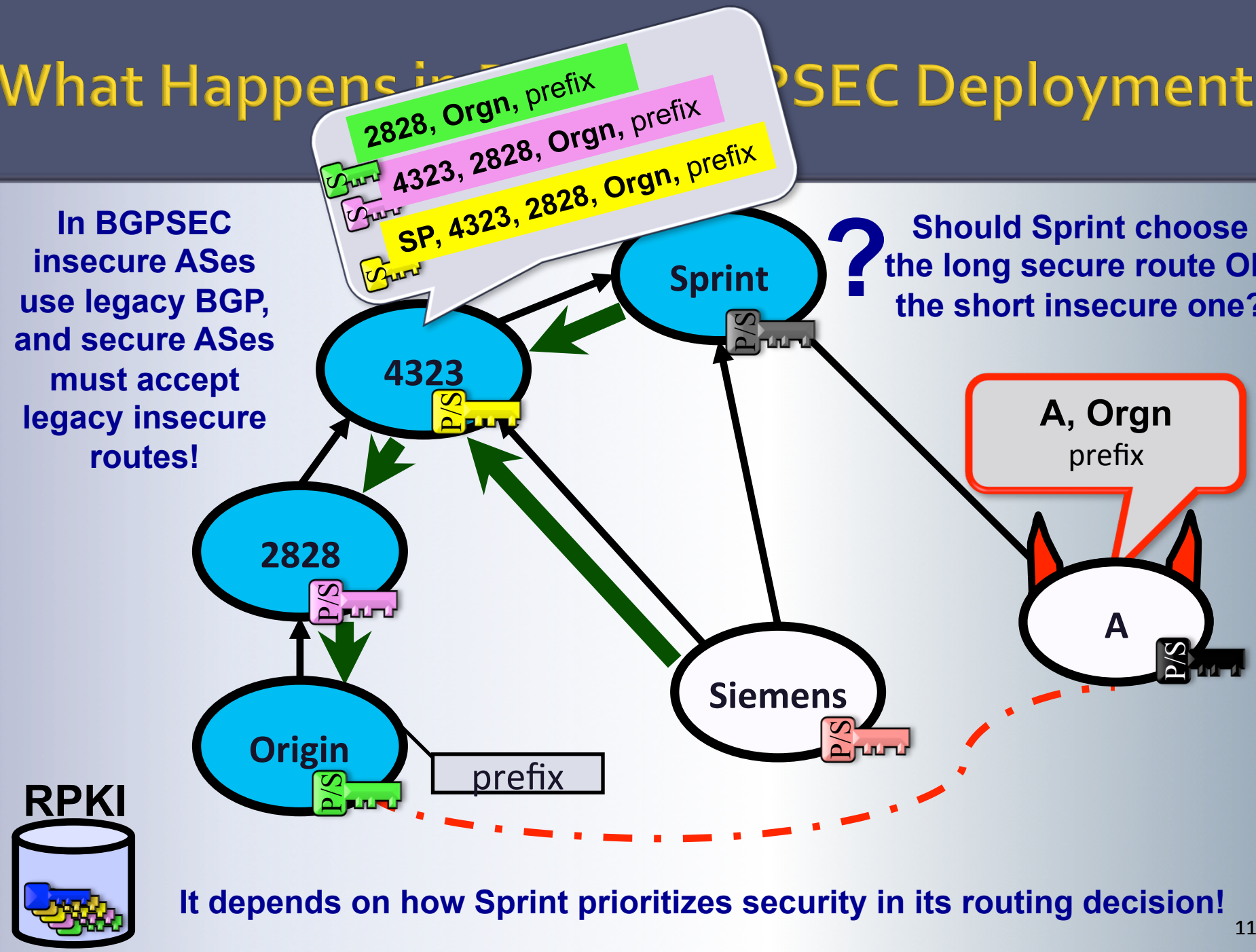
BGPSEC Pr… 1-Hop Hijack



Partial Landscape of BGP Defenses



What Happens in BGPSEC Deployment?



How to Prioritize Security?

1. local preference

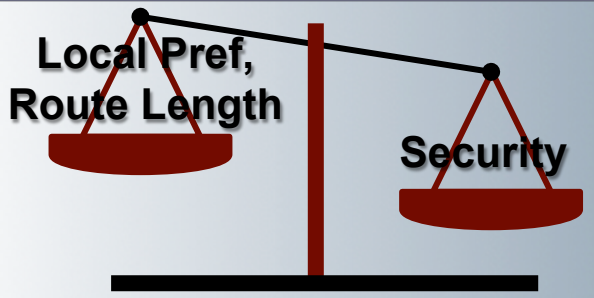
   (often based on business relationships with neighbors)

2. prefer short routes

   …

3. break ties in a consistent manner

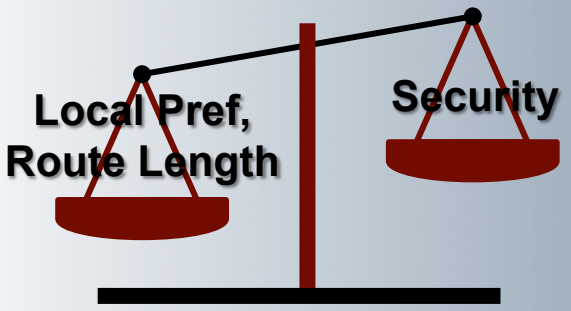
How to Prioritize Security?



→ **Security 1st**

1. local preference

   (often based on business relationships with neighbors)



→ **Security 2nd**

2. prefer short routes

→ **Security 3rd**

3. break ties in a consistent manner

✧ NANOG survey of 100 network operators shows that 10%, 20%, and 41% would place security 1st, 2nd, and 3rd respectively **[Gill, Schapira, Goldberg'12]**

Our Routing Model

→ **Security 1st**

1. local preference

   (prefer customer routes over peer over provider routes)

→ **Security 2nd**

2. prefer short routes

→ **Security 3rd**

3. break ties in a consistent manner

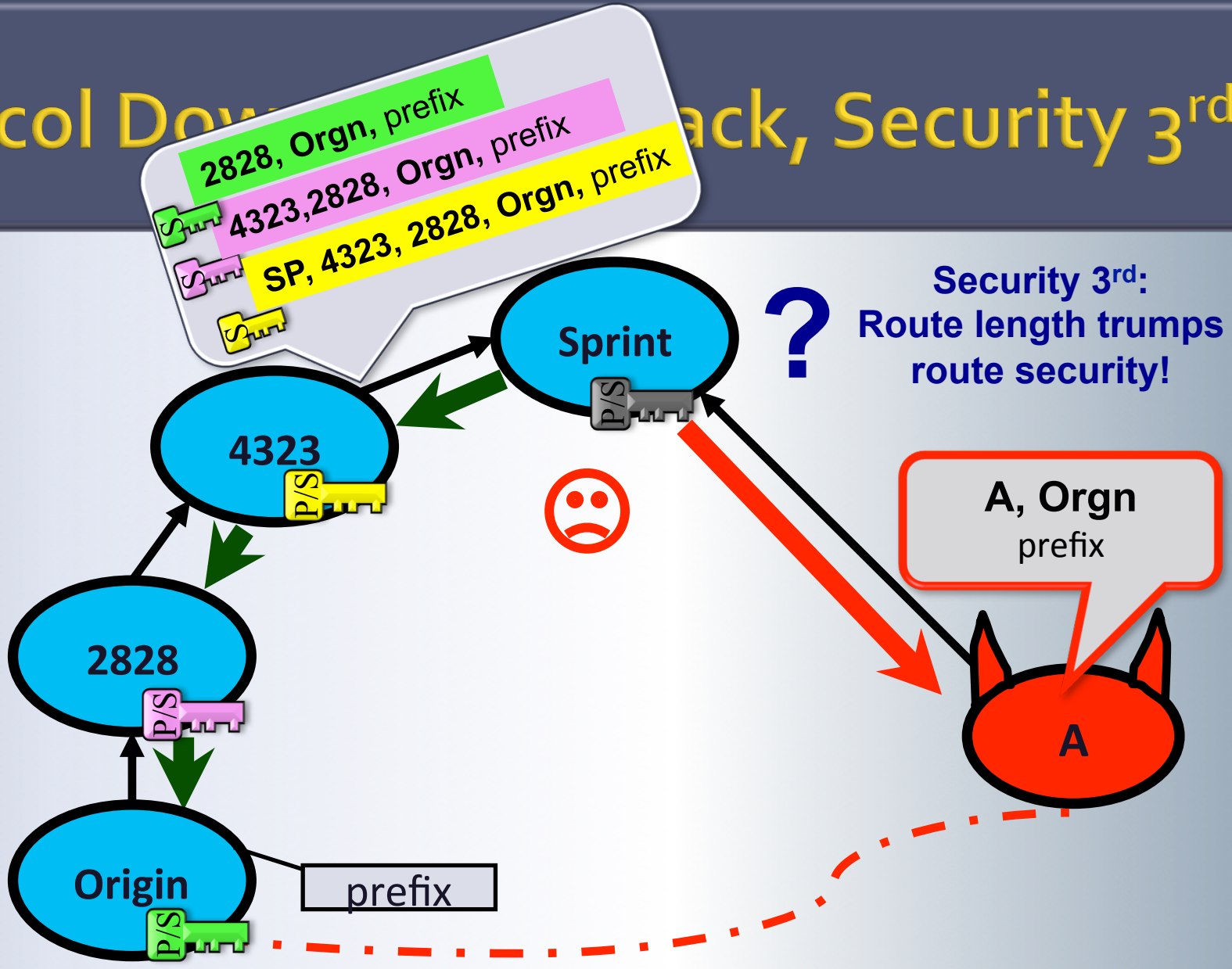
✧ To study routing outcomes, we use a concrete model of local preference. **[Gao-Rexford'00, Huston'99, etc.]**

✧ Our results are robust with respect to various local pref models

Outline

1. Background: BGP, RPKI, BGPSEC, routing policies
2. **BGPSEC in partial deployment is tricky**
    1. Protocol downgrade attacks
    2. Collateral damages
    3. Routing anomalies (Routing instabilities and BGP Wedgies)
3. Is the Juice worth the squeeze?
4. Summary

Protocol Dow…ack, Security 3rd!



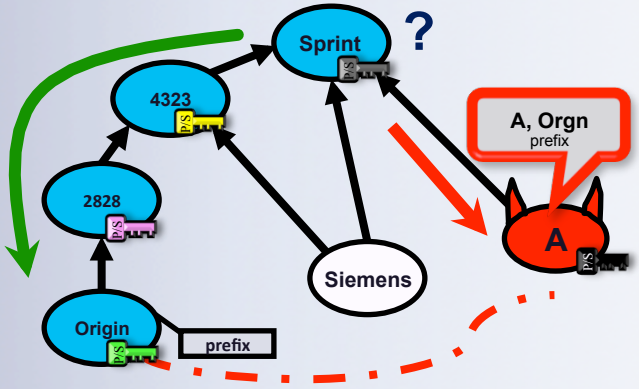
Protocol downgrade attack:

Before the attack, Sprint has a legitimate secure route.

During the attack, Sprint downgrades to an insecure bogus route .

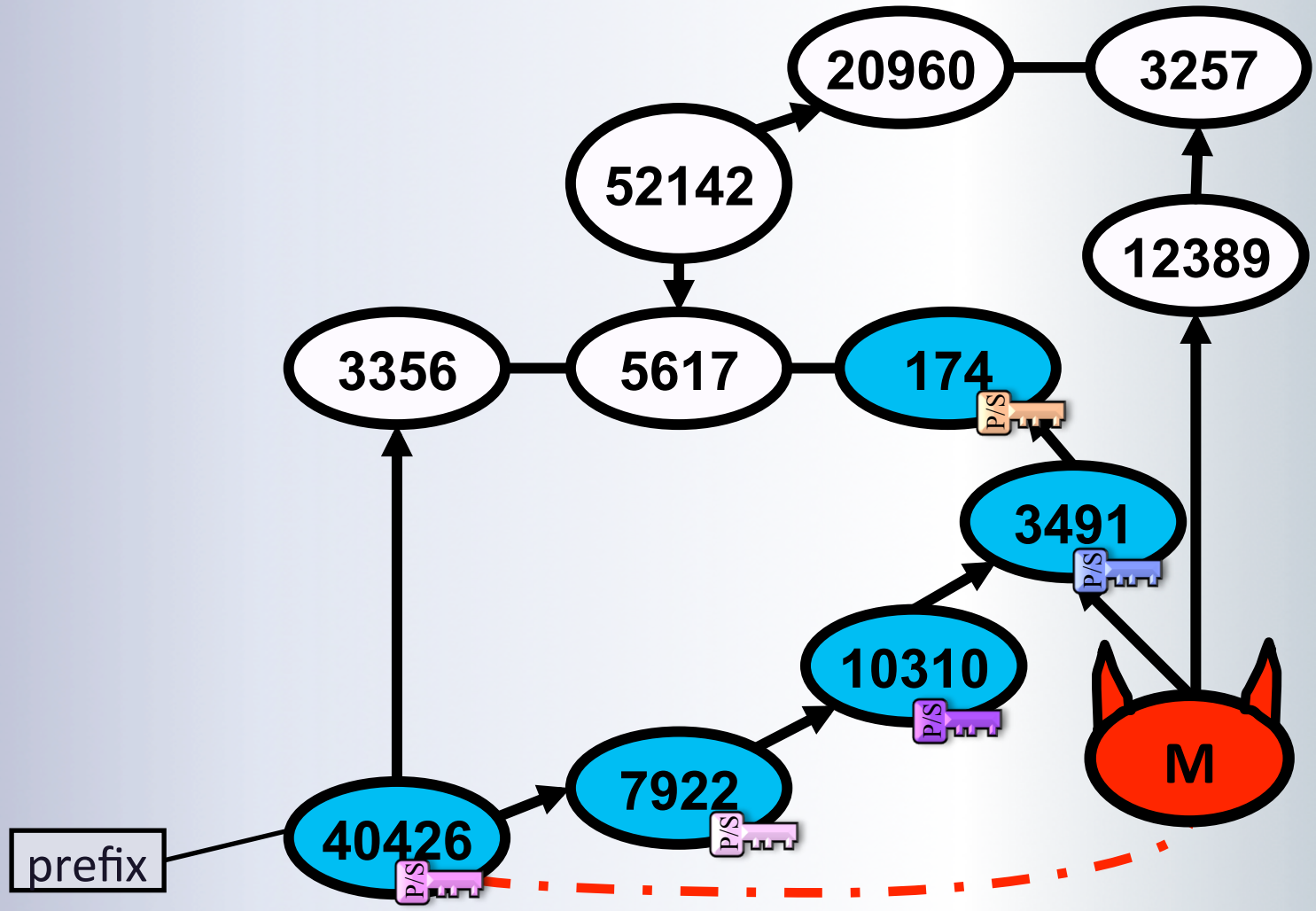
Partial Deployment is Very Tricky!

We prove…	No protocol downgrades?	No collateral damages?	No routing anomalies?
Security 1st	☺		
Security 2nd	☹		
Security 3rd	☹		

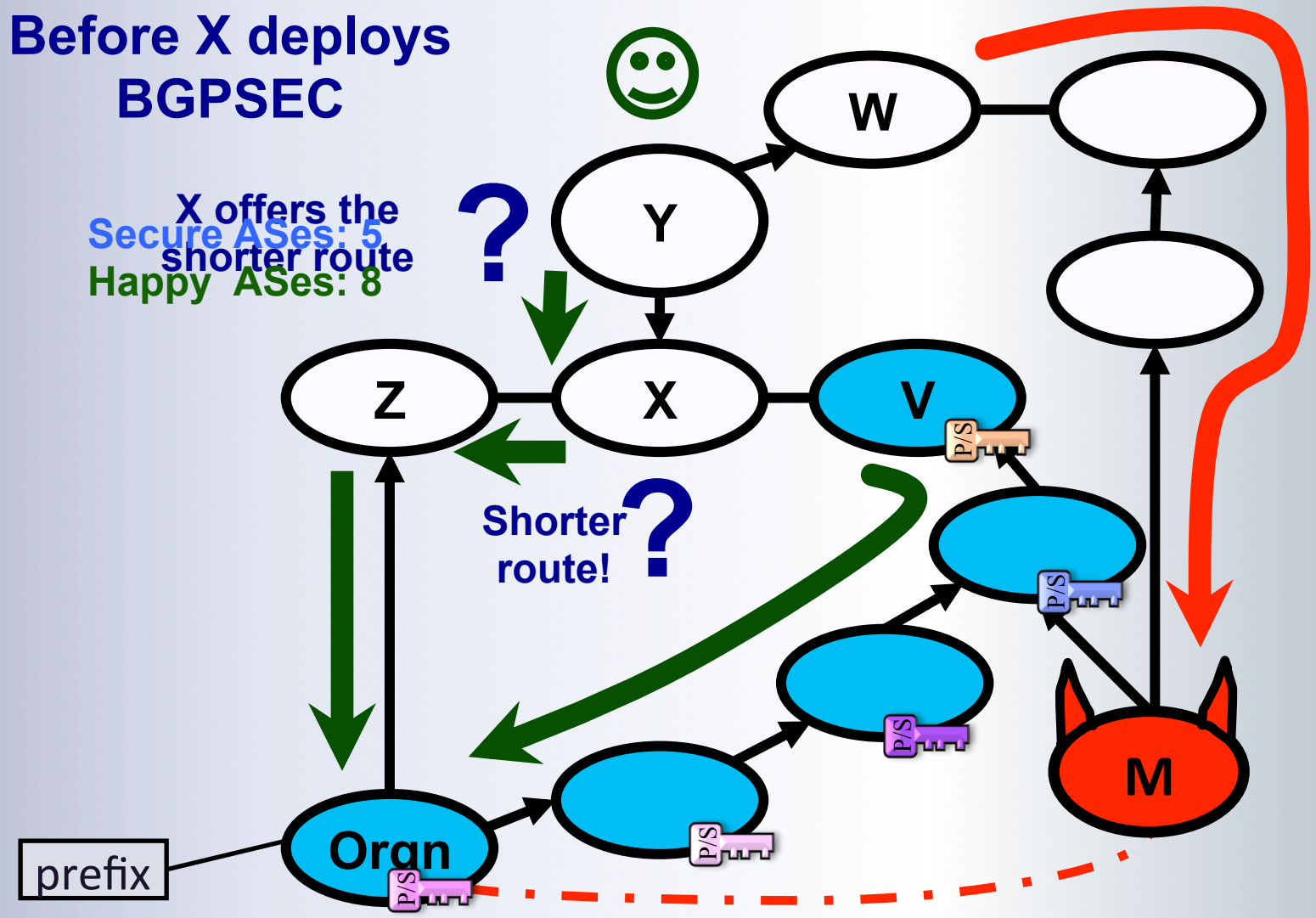


Protocol downgrade attack:
A secure AS with a secure route before the attack, downgrades to an insecure bogus route during the attack.

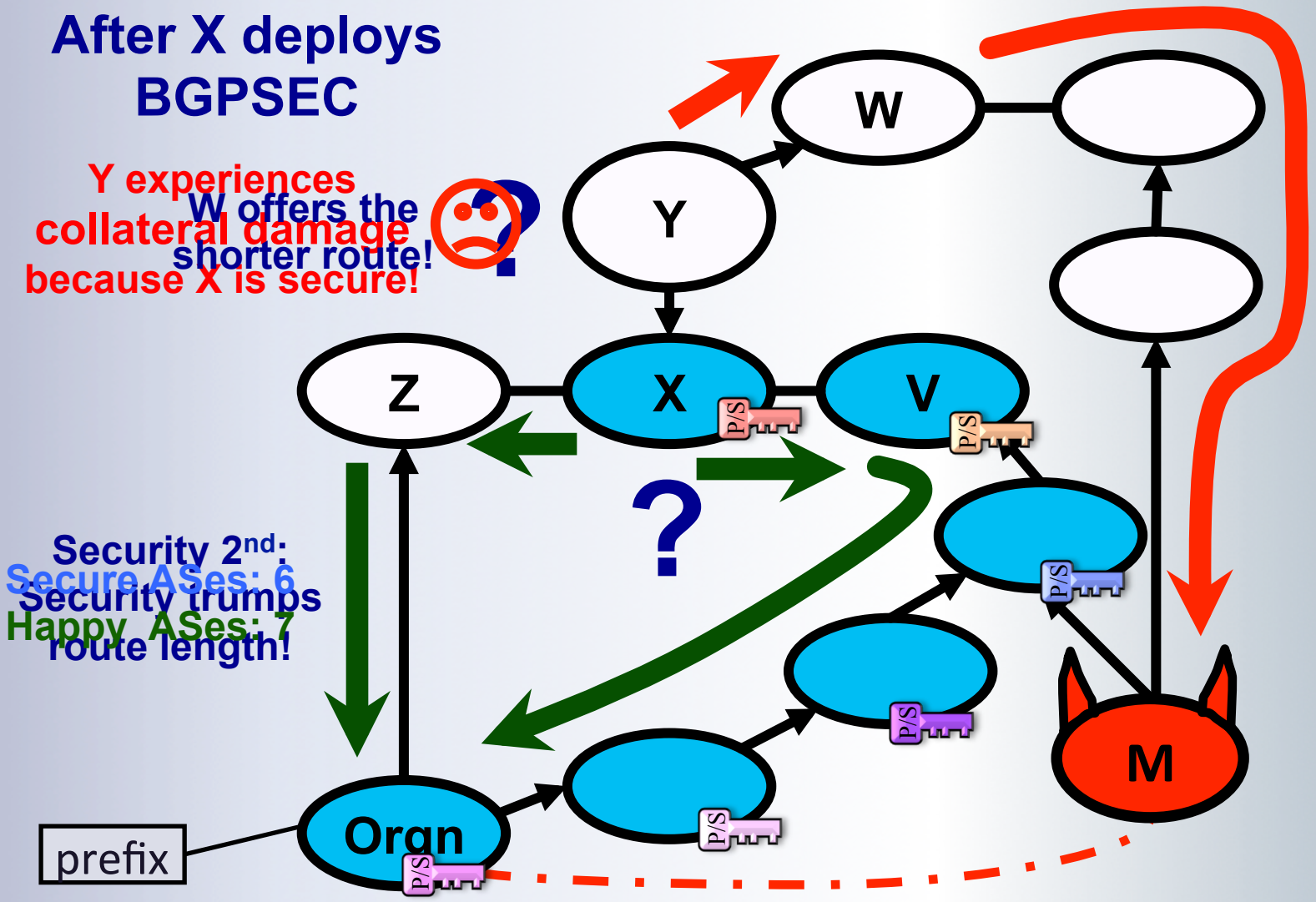
Collateral Damages; Security 2nd



Collateral Damages; Security 2nd

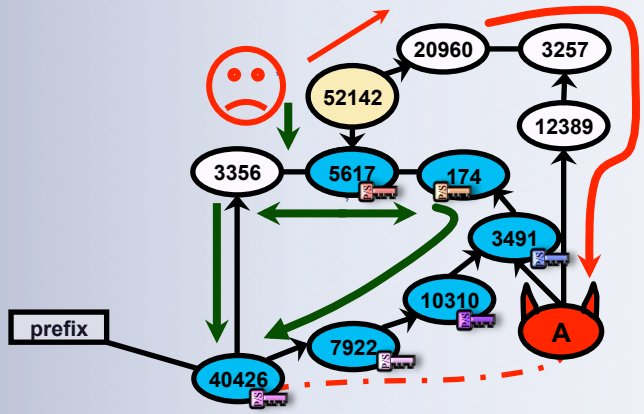


Collateral Damages; Security 2nd



Partial Deployment is Very Tricky!

We prove…	No protocol downgrades?	No collateral damages?	No routing anomalies?
Security 1st	☺	☹	
Security 2nd	☹	☹	
Security 3rd	☹	☺	



Collateral damage (during the attack):
More secure ASes leads to more insecure ASes choosing bogus routes

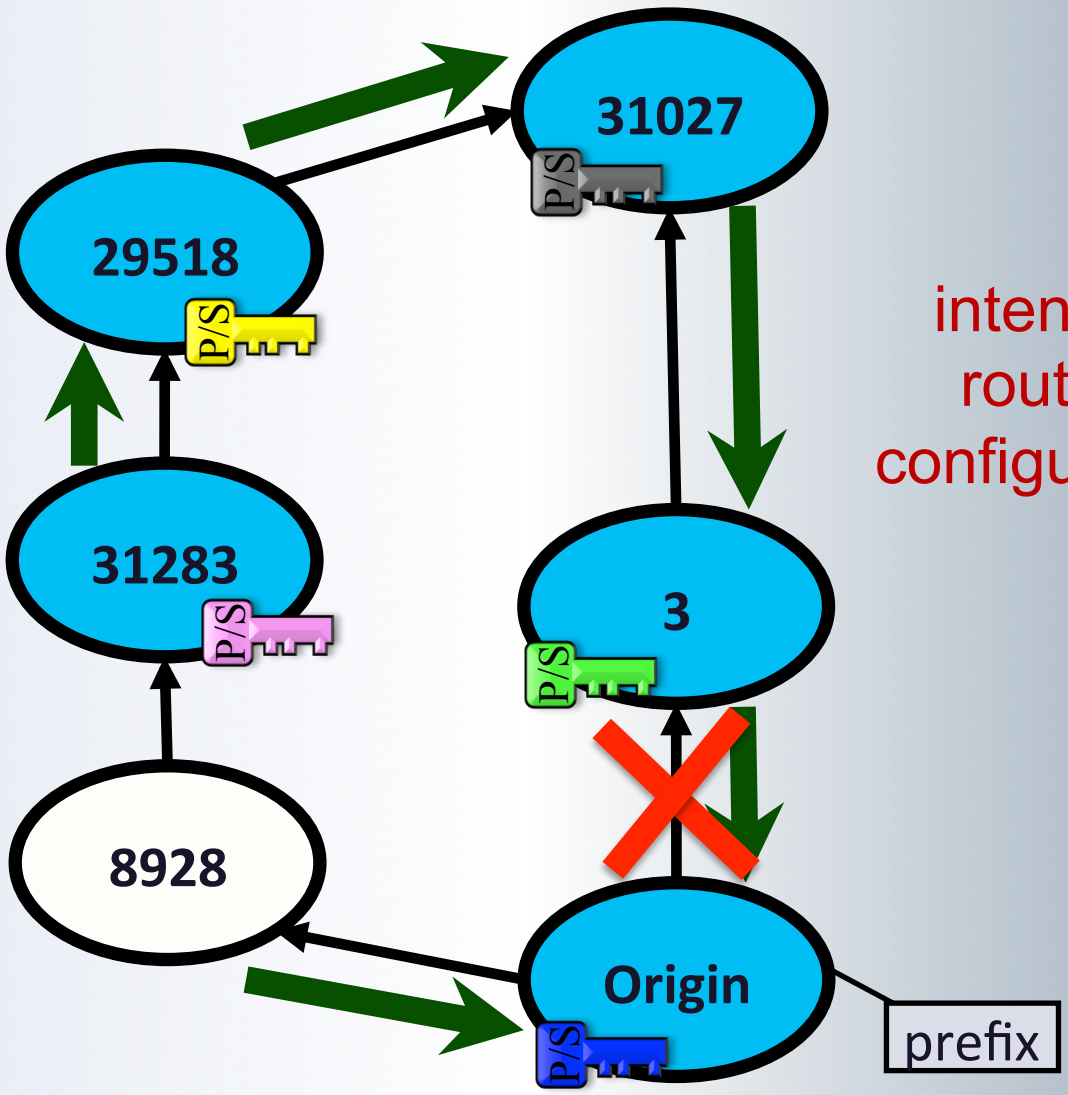
BGPSEC Wedgies

- Routing policies can also interact in ways that can cause BGP Wedgies **[Griffin and Huston, rfc-4264, 2005]**
  - can result in unpredictable and undesirable routing configurations

BGPSEC Wedgie

for 29518, local pref is more important than security

for 31283 security is more important than local pref

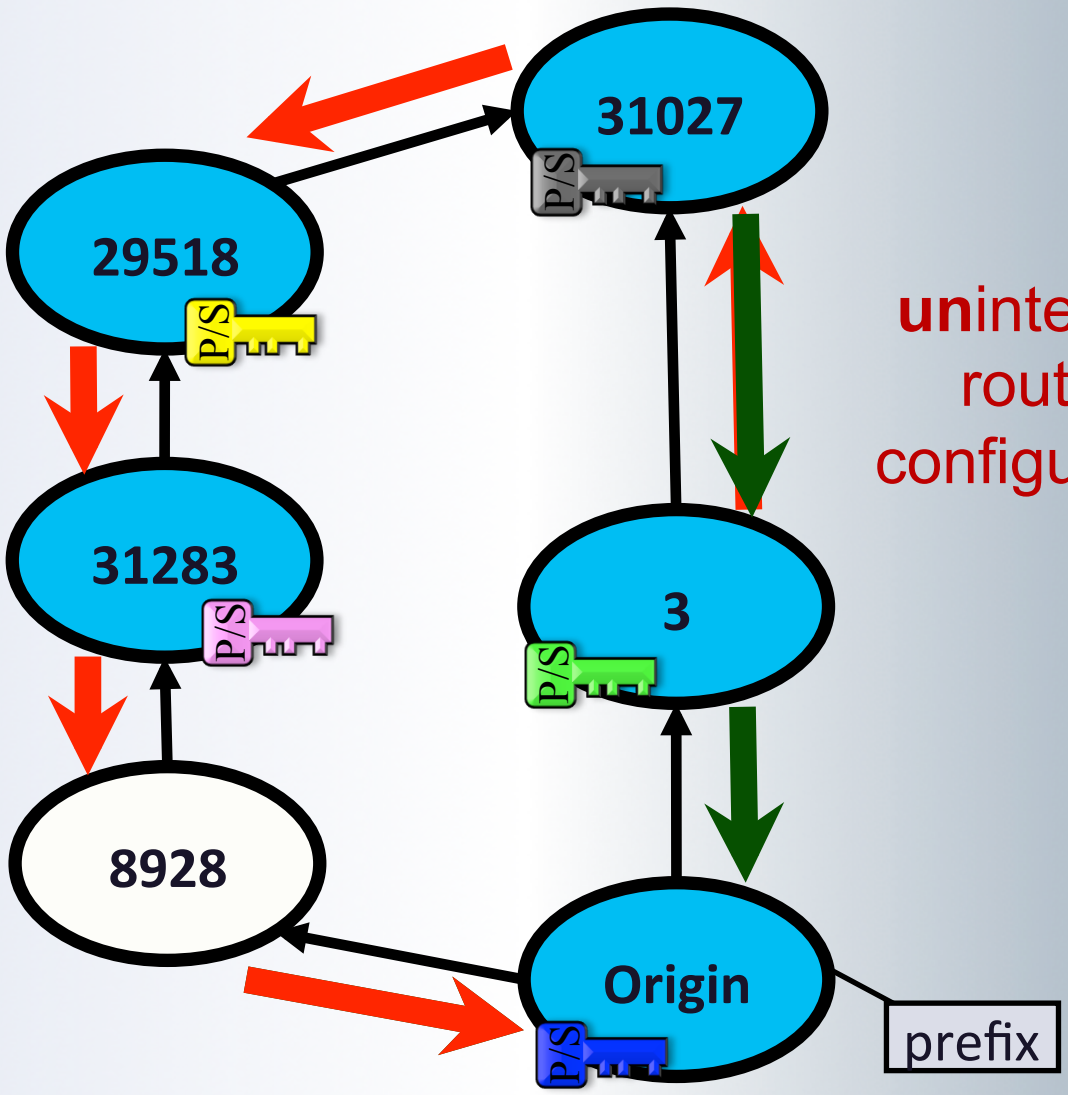


intended routing configuration

BGPSEC Wedgie

for 29518, local pref is more important than security

for 31283 security is more important than local pref



unintended routing configuration

Partial Deployment is Very Tricky!

We prove…	No protocol downgrades?	No collateral damages?	No routing anomalies?
Security 1st	☺	☹	☺
Security 2nd	☹	☹	☺
Security 3rd	☹	☺	☺

Routing anomalies such as BGPSEC Wedgies and persistent routing oscillations and can be avoided as long as all ASes prioritize security the same way.

Otherwise, these routing anomalies could happen.

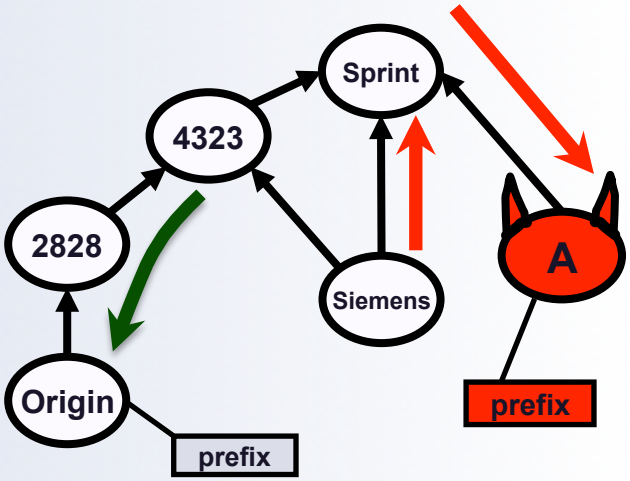
Outline

1. Background: BGP, RPKI, BGPSEC, routing policies
2. BGPSEC in partial deployment is tricky
3. **Is the Juice worth the Squeeze?**
    1. How can we quantify BGPSEC benefits?
    2. Can we bound BGPSEC benefits without knowing who may deploy it?
    3. What are BGPSEC benefits beyond what RPKI can provide?
4. Summary

How to Quantifying BGPSEC Benefits?

Fix a particular Origin, attacker A and

let S be the set of ASes deploying BGPSEC



$S = \emptyset$

$|\text{Happy}(S, A, \text{Origin})| = 3$

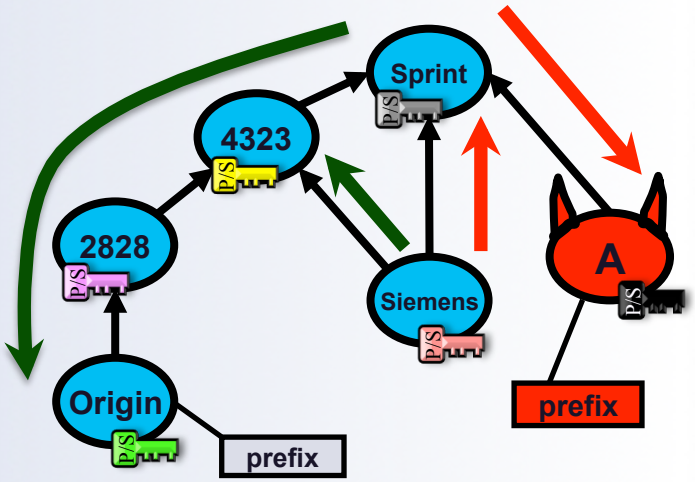
The set of ASes choosing a legitimate route is

$$\text{Happy}\left[S, A, \text{Origin}\right]$$

How to Quantify BGPSEC Benefits?

Fix a particular Origin, attacker A and

let S be the set of ASes deploying BGPSEC



S = everyone

$|\text{Happy}(S, A, \text{Origin})| = 5$

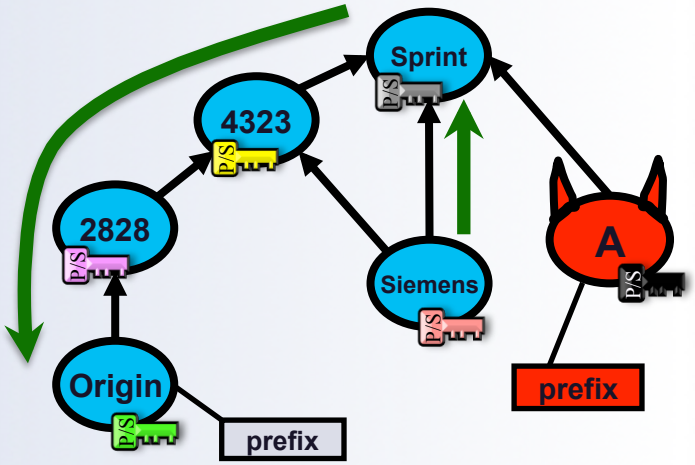
The set of ASes choosing a legitimate route is

$$\text{Happy}\left[S, A, \text{Origin} \rightarrow \text{prefix}\right]$$

Quantifying Security: A Metric

Fix a particular Origin, attacker A and

let S be the set of ASes deploying BGPSEC



S = everyone

$$\left| \text{Happy}(S, A, \text{Origin}) \right| = 5$$

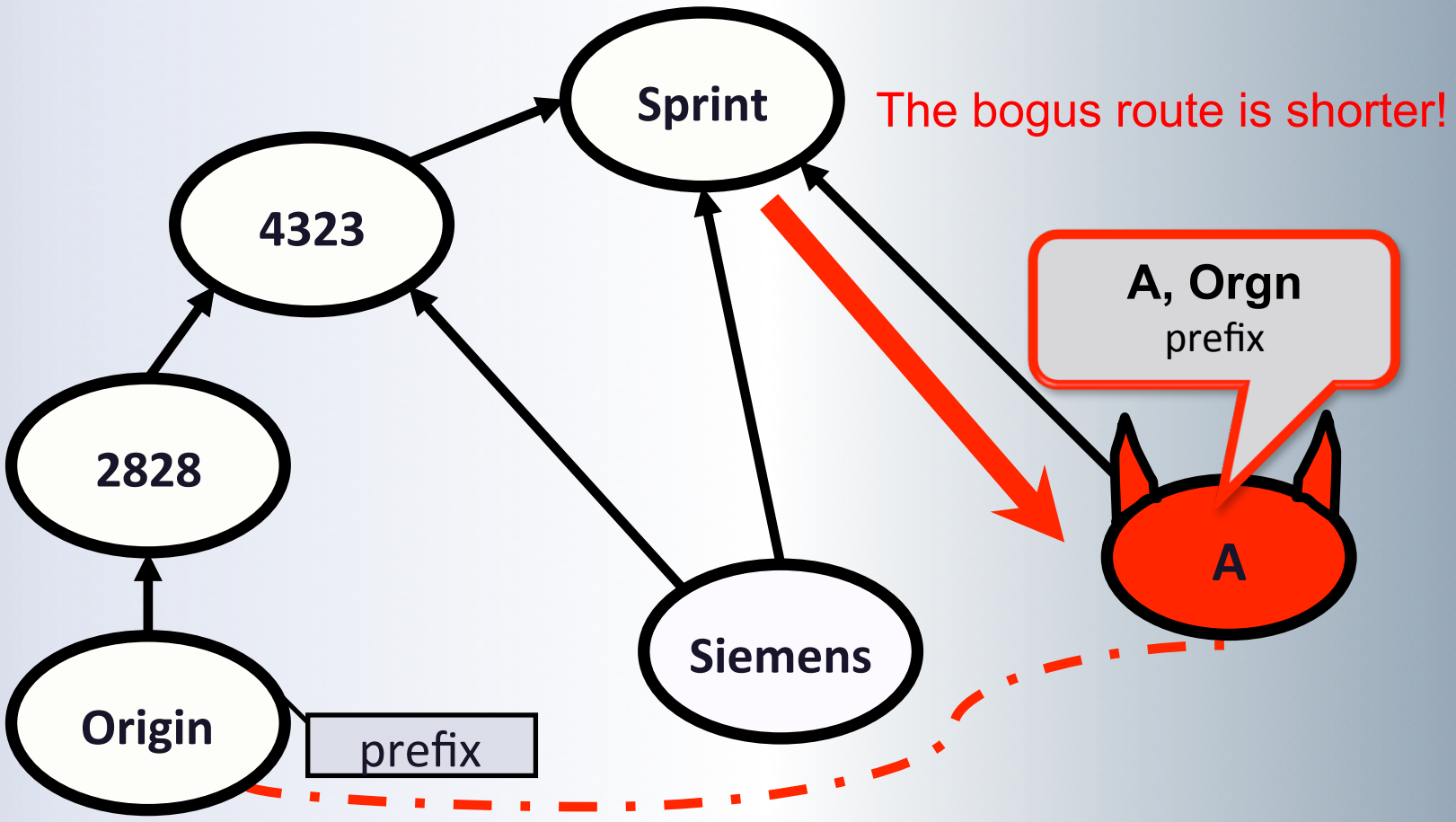
Our metric is the average of the set of Happy ASes

$$\text{Metric}(S) = \frac{1}{|V|^3} \sum_{\substack{\text{all } A \\ \text{all O}}} \left| \text{Happy}\left[S, A, \text{Origin} \right] \right|$$

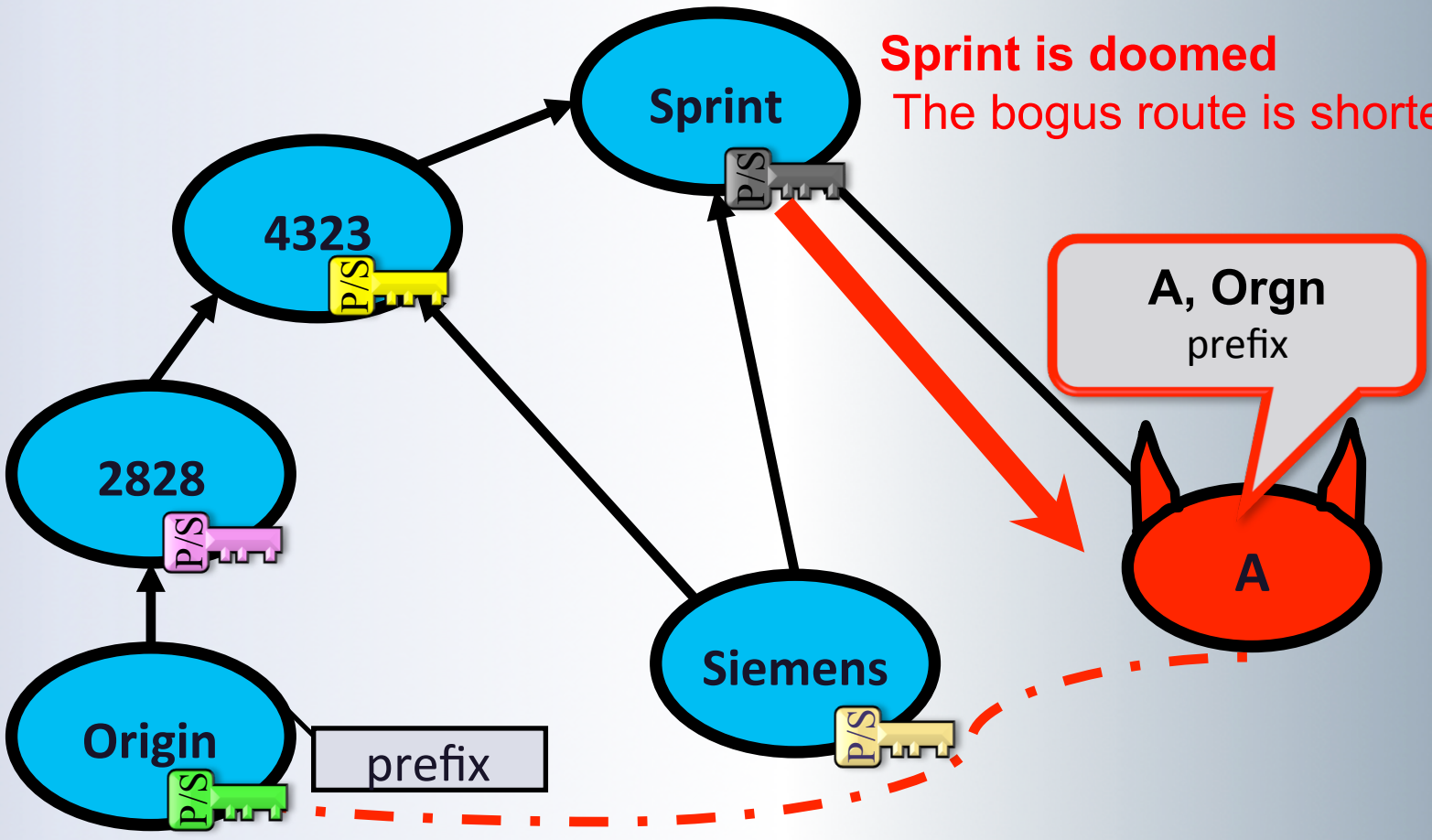
Who Should Deploy BGPSEC?

- We can efficiently compute bounds on BGPSEC benefits independently of who deploys it
  - to do this we figure out which ASes do not benefit from BGPSEC by considering only the scenario when no AS deploys BGPSEC

Bounding BGPSEC Benefits: Security 3rd

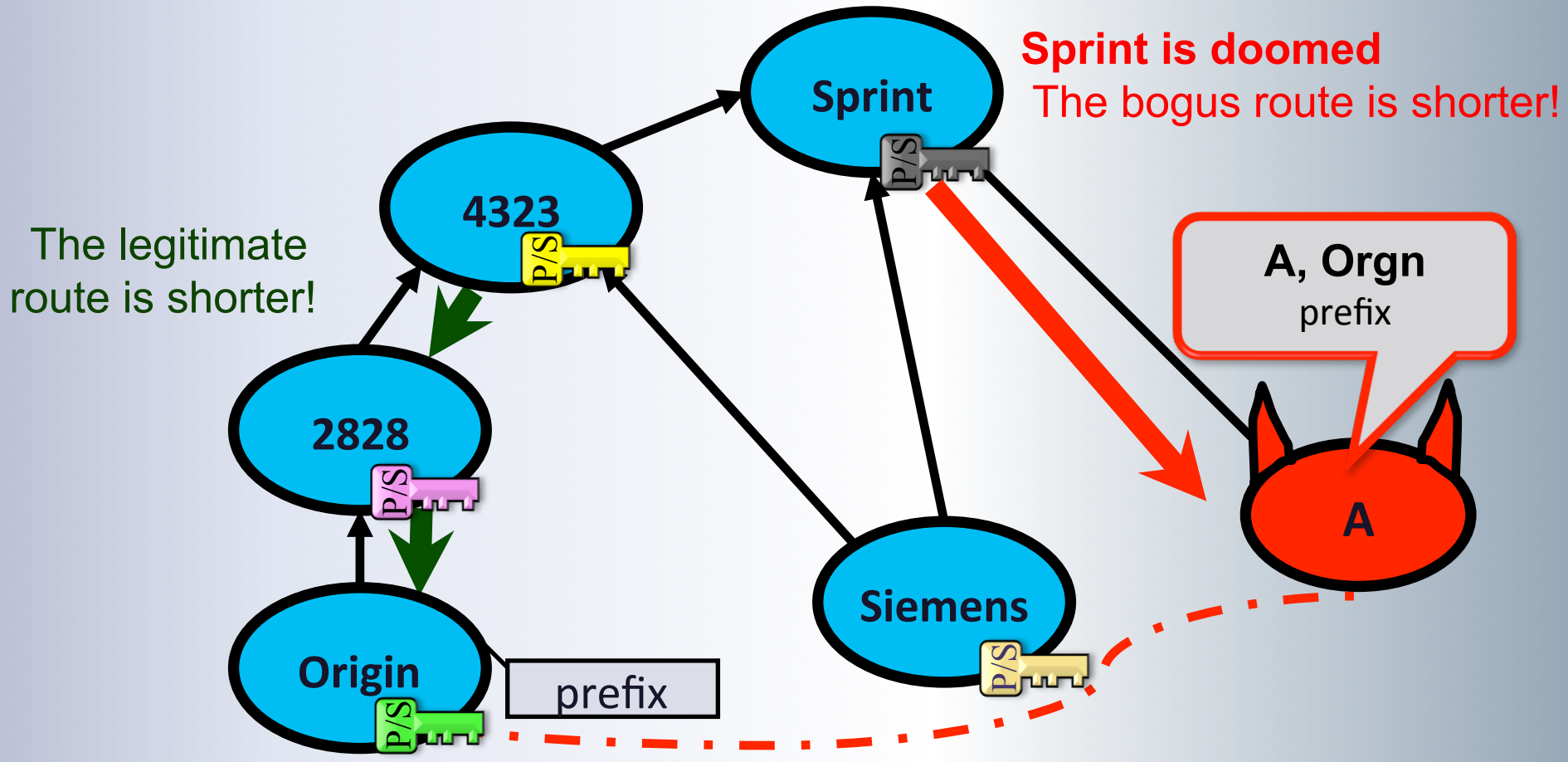


Bounding BGPSEC Benefits: Security 3rd

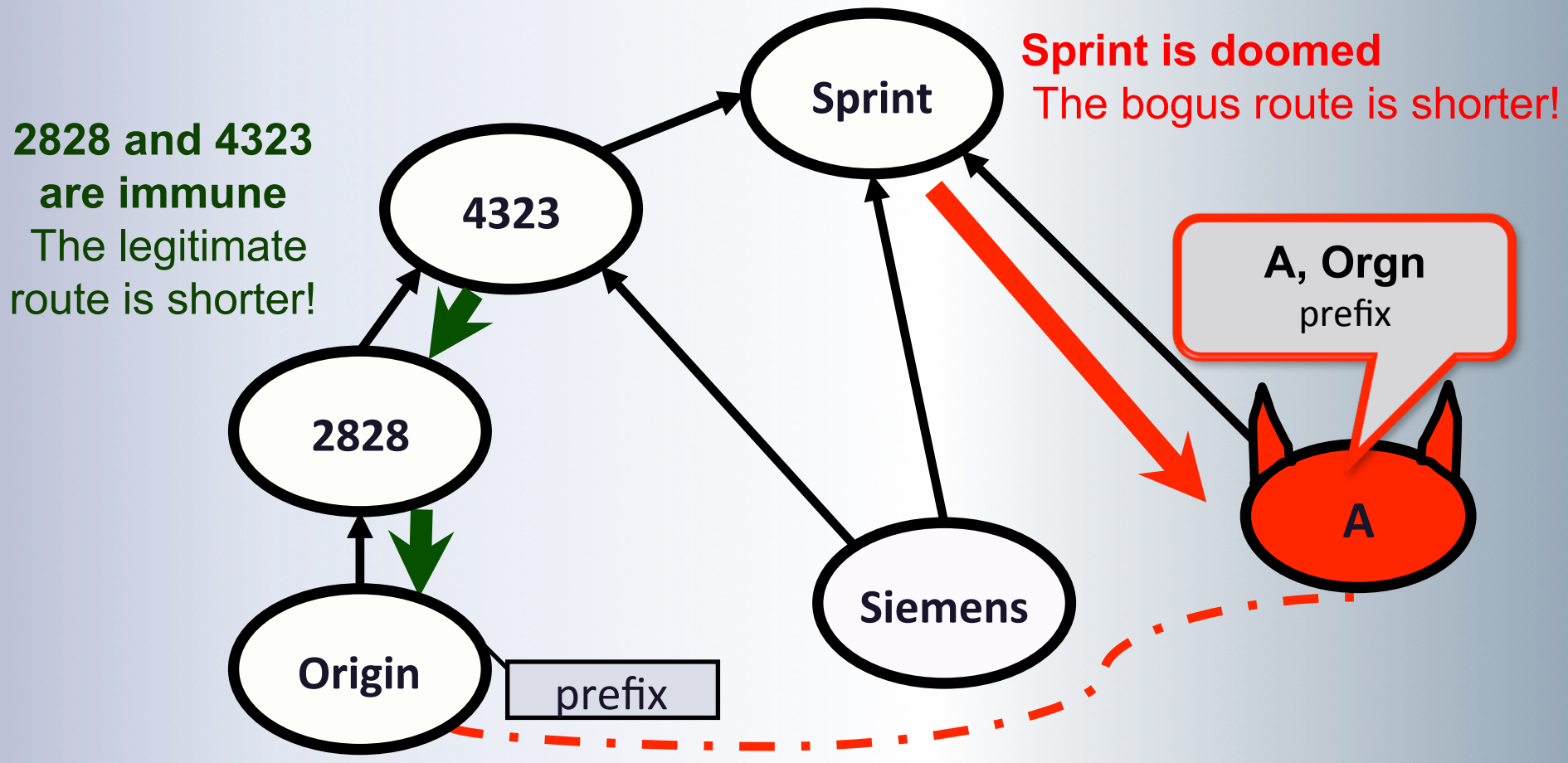


Regardless of who is secure, Sprint will select the shorter bogus route!

Bounding BGPSEC Benefits: Security 3rd

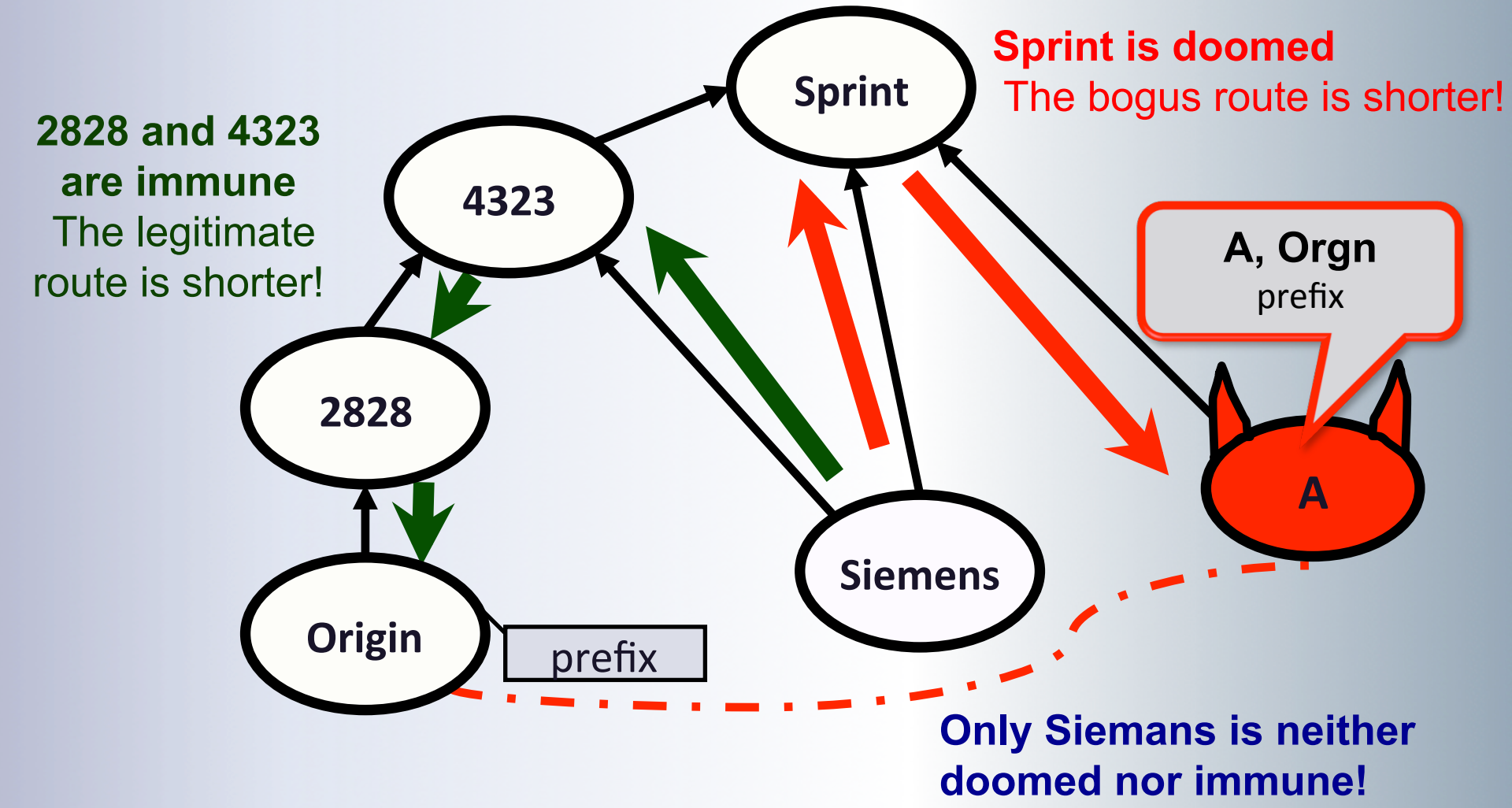


Bounding BGPSEC Benefits: Security 3rd

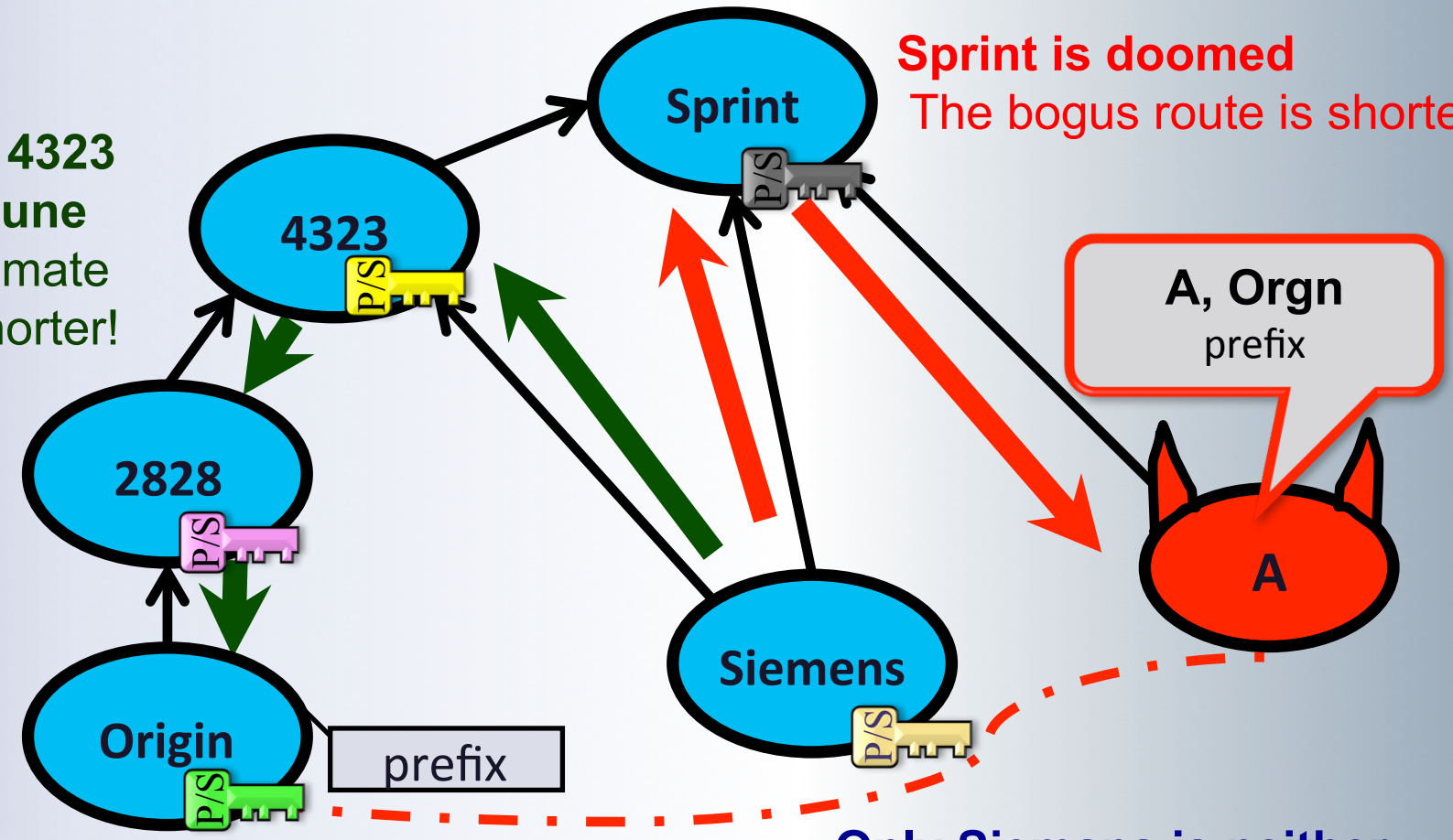


Regardless of who is secure, 4323 and 2828 will select legitimate routes!

Bounding BGPSEC Benefits: Security 3rd



Bounding BGPSEC Benefits: Security 3rd



2828 and 4323 are immune
The legitimate route is shorter!

Sprint is doomed
The bogus route is shorter!

Only Siemans is neither doomed nor immune!

Regardless of who is secure, only Siemans can benefit from BGPSEC!

Quantifying BGPSEC Benefits

✧ Regardless of who deploys BGPSEC:

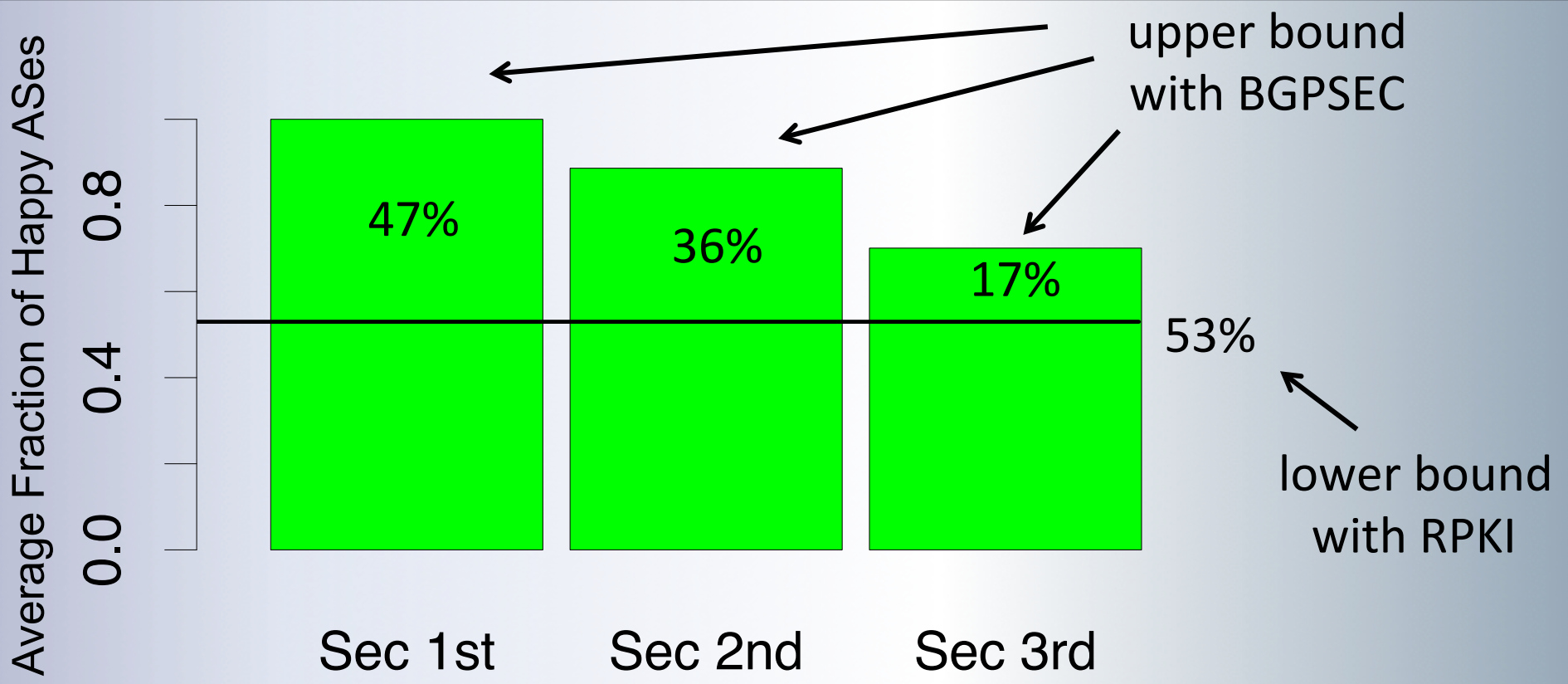
1. **Doomed ASes** will always choose bogus routes
2. **Immune ASes** will always choose legitimate routes
3. Only **protectable** ASes can be benefit from BGPSEC

✧ Security benefits **lower** bound = fraction of **immune** ASes

✧ Security benefits **upper** bound = 1 - fraction of **doomed** ASes

✧ Most ASes are immune or doomed when security is 3rd

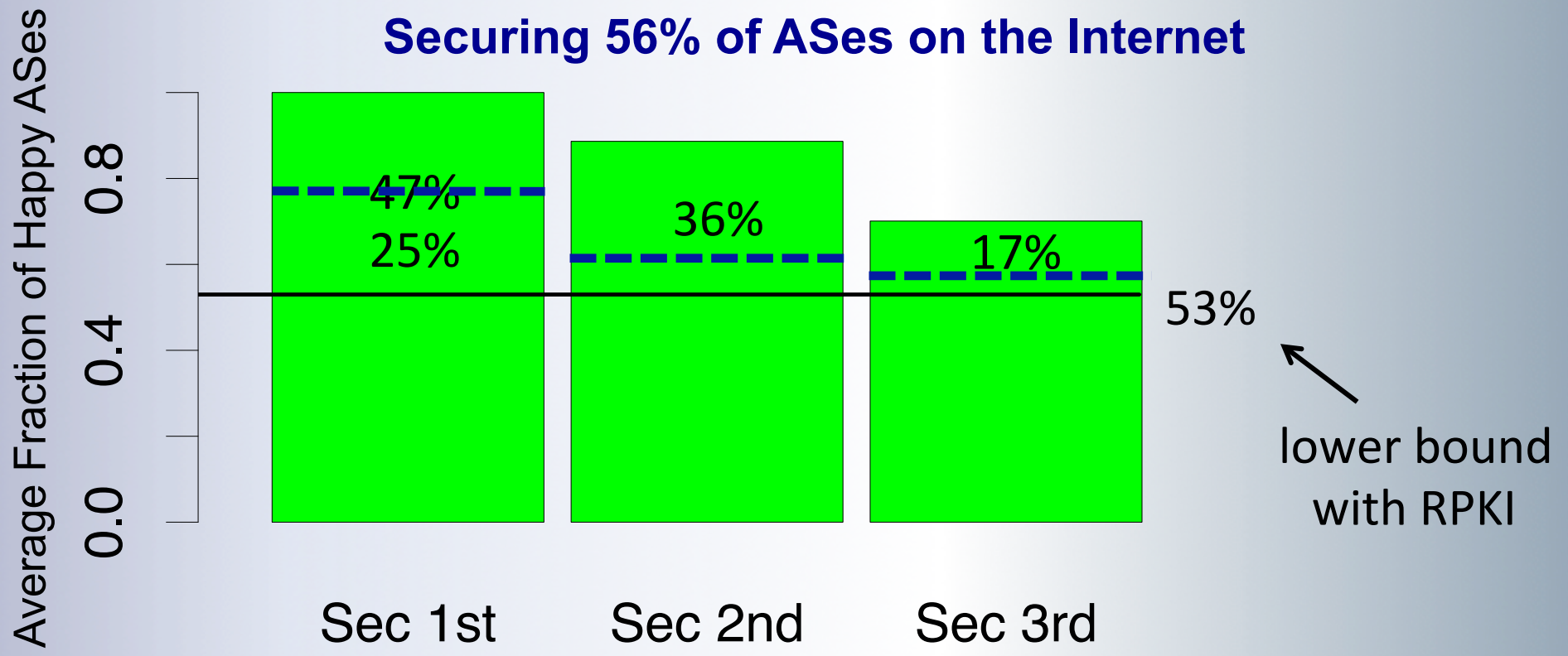
BGPSEC Benefits Bounds over RPKI



In the most realistic security 3rd model, the best we could do is make extra 17% happy with security!

Securing 213 High Degree ASes & their Stubs

(13 Tier 1's + 100 Tier 2's + 100 Tier 3's + all their stubs)



Improvements in the security 3rd and 2nd models are only 5% and 10% respectively.

Our Methodology

- Graph: A UCLA AS-level topology from 09-24-2012
  - 40K ASes, 73.5K and 62K customer-provider and peer links
- Used large-scale simulations to determine
  - upper and lower bounds on metric improvement
  - security-benefits for many different BGPSEC deployments
- Robustness Tests
  - added 550K extra peering links inferred from IXP data on 09-24-2012
  - accounted for traffic patterns by focusing on only certain destinations (e.g. content providers) and attackers
  - repeated analysis with respect to different local pref models

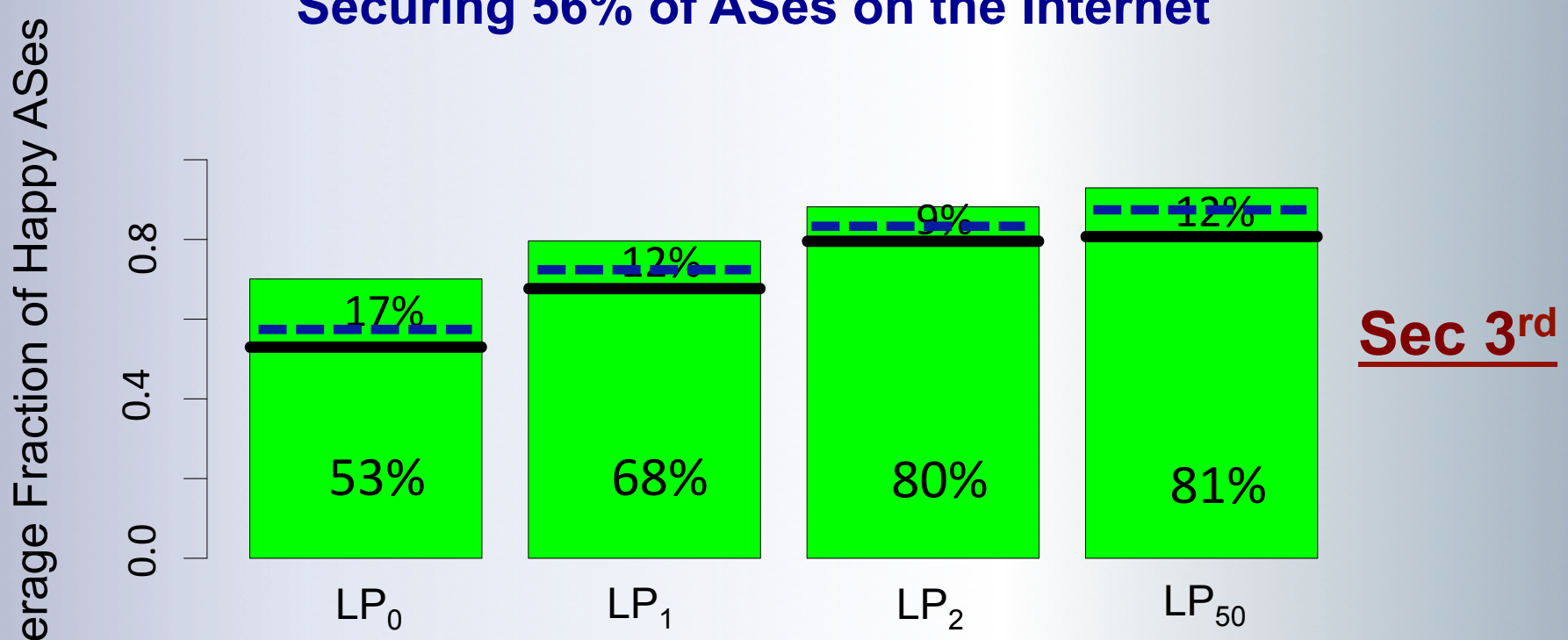
The LP_k Local Pref Model

- Survey shows ~80% of network operators prefer customer over peer routes, but some (e.g. content providers) prefer shorter peer routes over longer customer routes **[Gill, Schapira, Goldberg 2012]**

- In the **LP_k** model, for any $k \geq 0$, rank routes as follows:
  - customer routes of length 1
  - peer routes of length 1
  - …
  - customer routes of length k
  - peer route of length k
  - customer routes of length > k
  - peer routes of length > k
  - provider routes

Securing 213 High Degree ASes & their Stubs

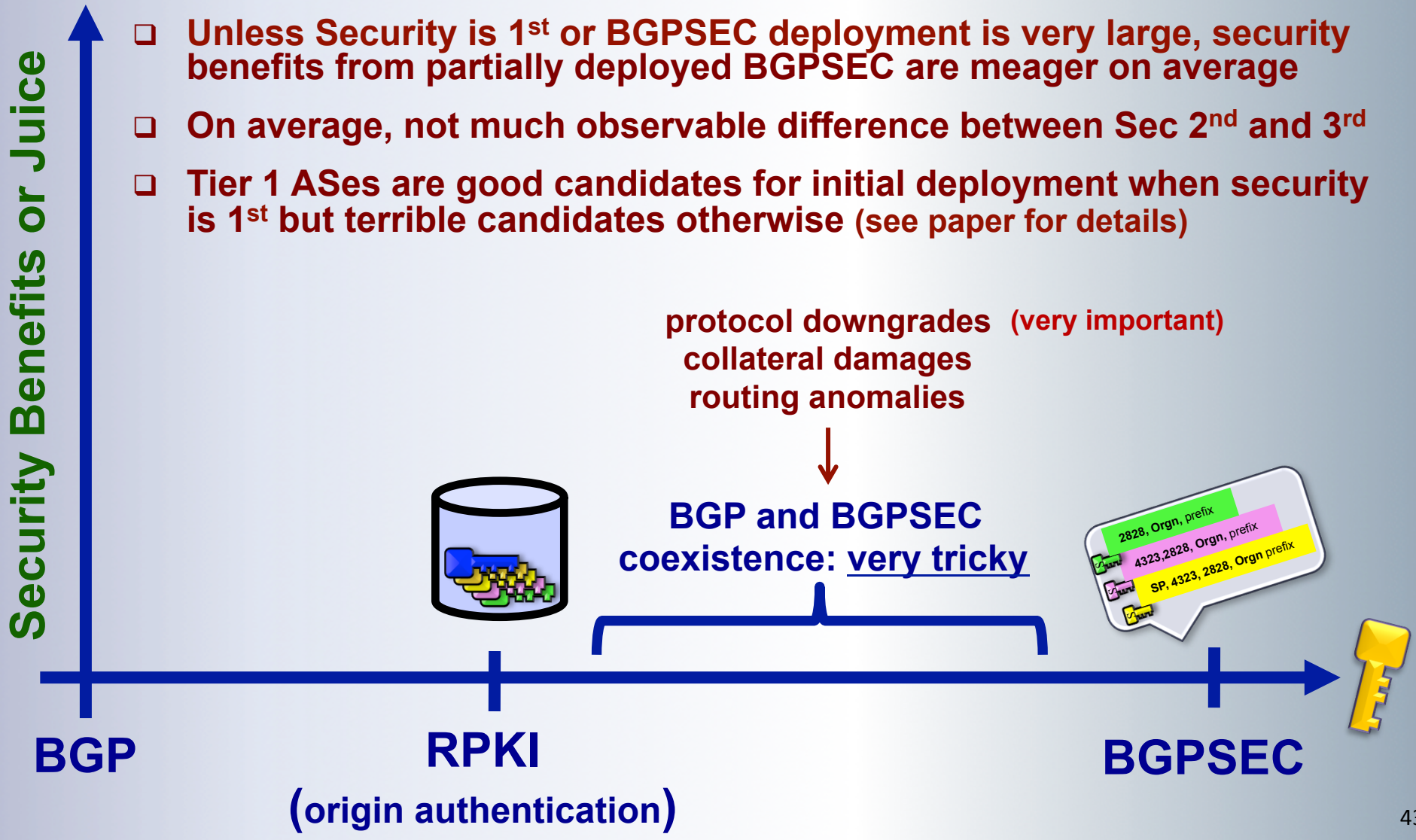
(13 Tier 1's + 100 Tier 2's + 100 Tier 3's + all their stubs)



As *k* increases, metric improvements are 5%, 4%, 4%, and 6%.

So Is the Juice Worth the Squeeze?

- Unless Security is 1st or BGPSEC deployment is very large, security benefits from partially deployed BGPSEC are meager on average
- On average, not much observable difference between Sec 2nd and 3rd
- Tier 1 ASes are good candidates for initial deployment when security is 1st but terrible candidates otherwise (see paper for details)



THANK YOU

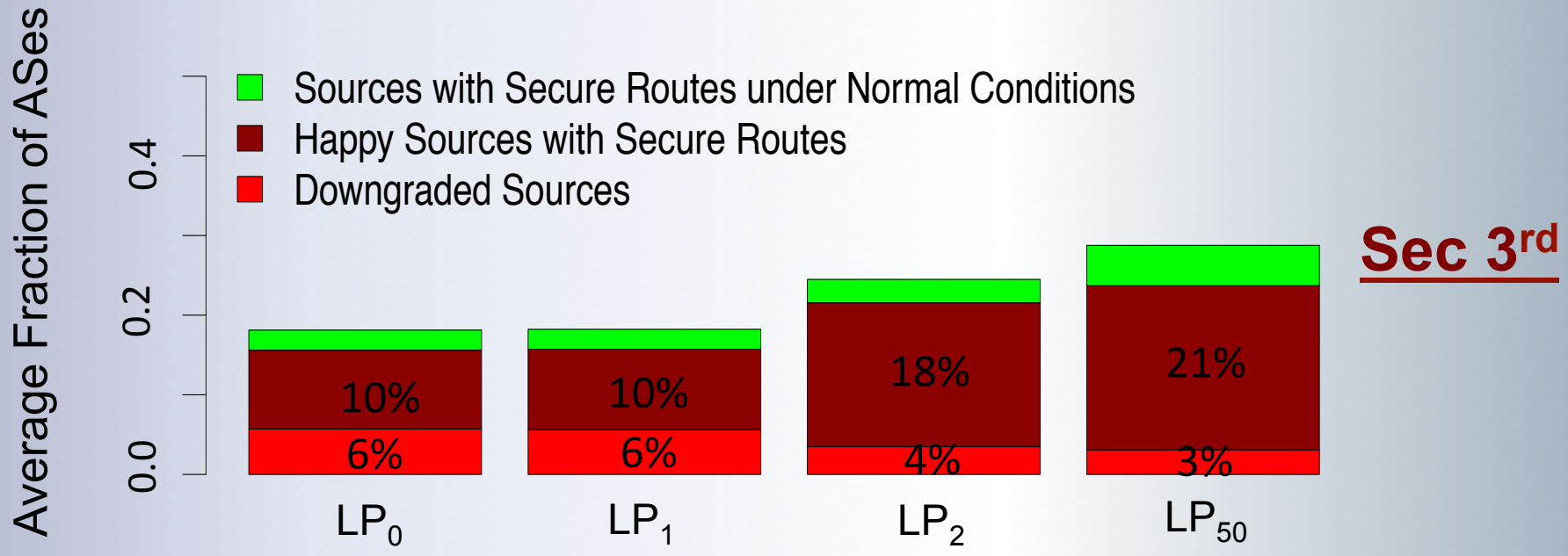
check out the full version at
http://arxiv.org/abs/1307.2690

1. **More empirical analysis and plots**
2. **More Robustness tests**
3. **BGPSEC deployment guidelines**

Securing 213 High Degree ASes & their Stubs

(13 Tier 1's + 100 Tier 2's + 100 Tier 3's + all their stubs)

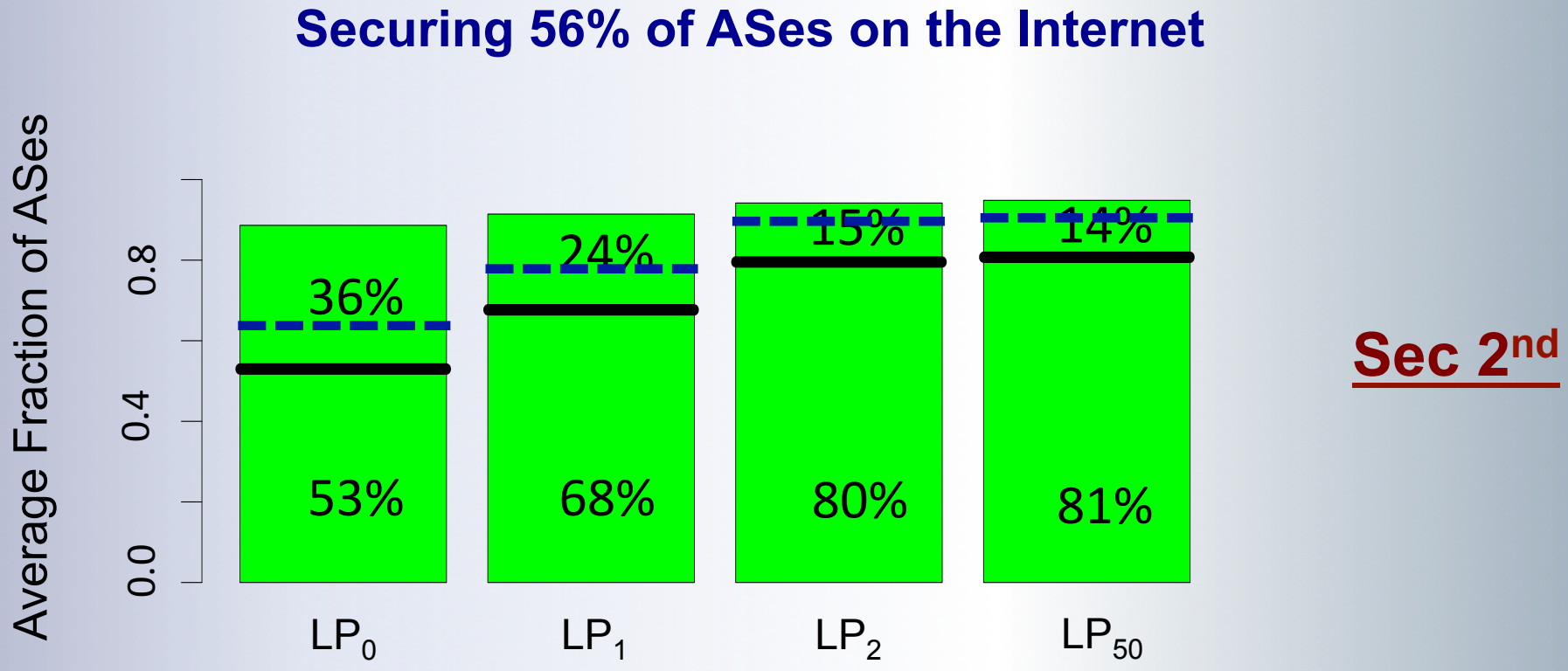
Securing 56% of ASes on the Internet



As *k* increases, the fraction of ASes with secure routes grows, but most of them are happy anyway.

Securing 213 High Degree ASes & their Stubs

(13 Tier 1's + 100 Tier 2's + 100 Tier 3's + all their stubs)

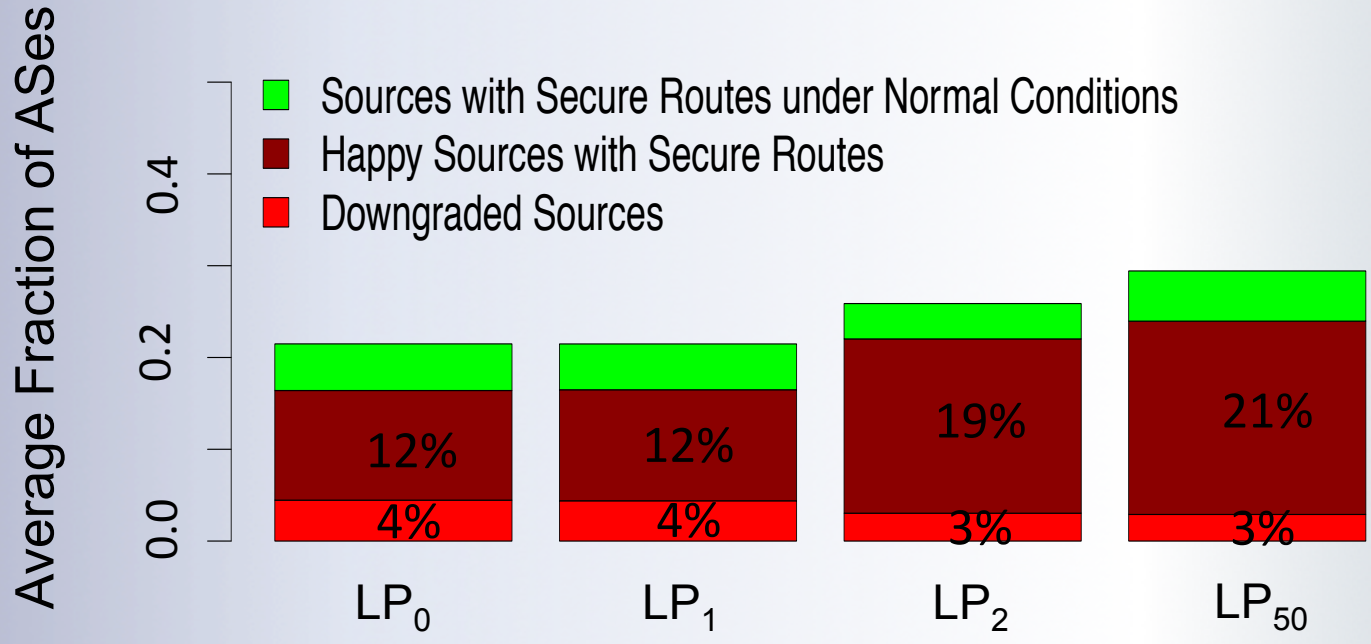


As ASes become more stubborn (i.e. *k* increases), metric improvements are 9.9%, 9.7%, 10.1%, and 9.8%

Securing 213 High Degree ASes & their Stubs

(13 Tier 1's + 100 Tier 2's + 100 Tier 3's + all their stubs)

Securing 56% of ASes on the Internet



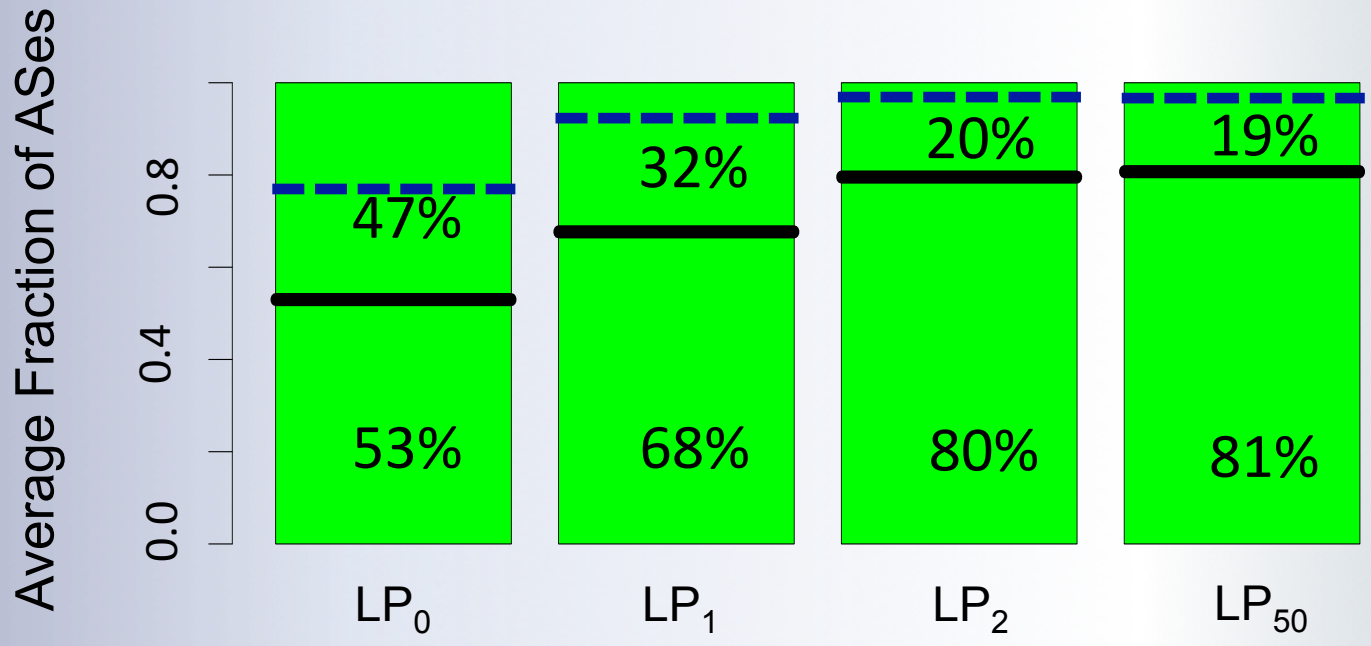
Sec 2nd

As ASes become more stubborn (i.e. *k* increases), fraction of ASes with secure routes grows, but most of them are happy anyway

Securing 213 High Degree ASes & their Stubs

(13 Tier 1's + 100 Tier 2's + 100 Tier 3's + all their stubs)

Securing 56% of ASes on the Internet



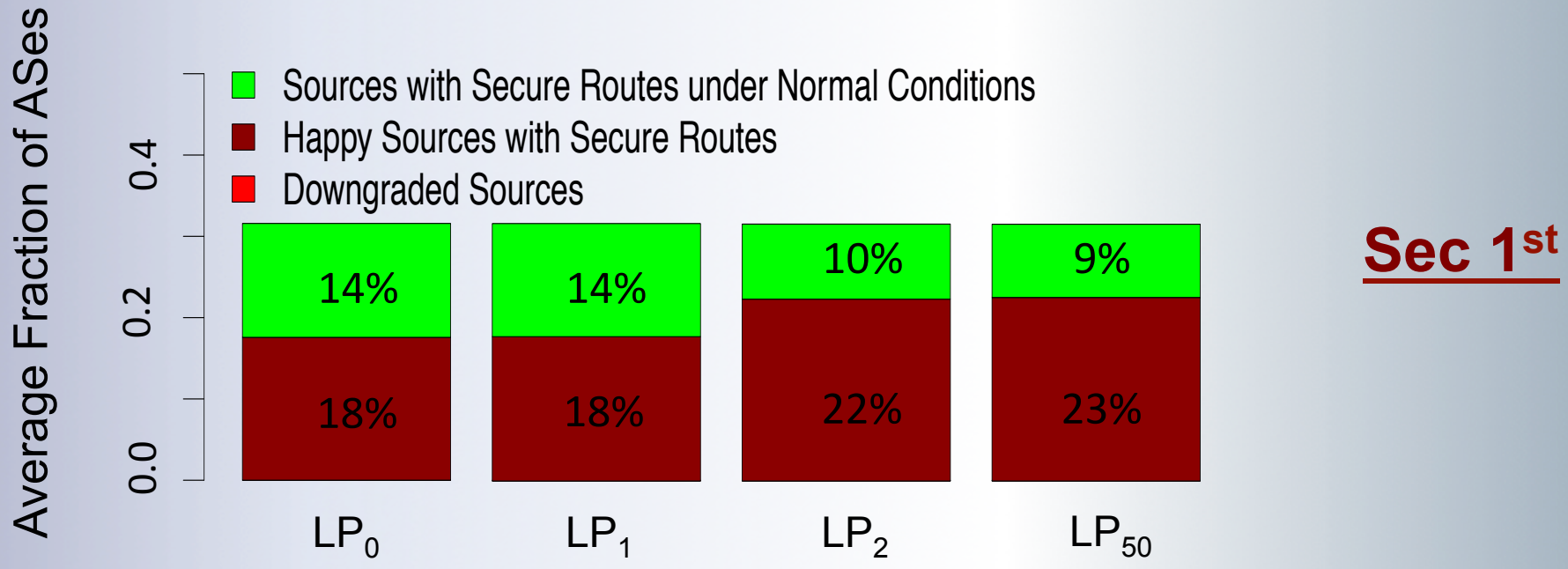
Sec 1st

As ASes become more stubborn (i.e. *k* increases), metric improvements are 24.8%, 24.7%, 17.2%, and 16.1%

Securing 213 High Degree ASes & their Stubs

(13 Tier 1's + 100 Tier 2's + 100 Tier 3's + all their stubs)

Securing 56% of ASes on the Internet



Sec 1st

As ASes become more stubborn (i.e. *k* increases), fraction of happy ASes with secure routes grows