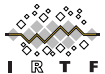
Applied Networking Research Workshop 2020



Limiting the Power of RPKI Authorities

Kris Shrishak Haya Shulman

TU Darmstadt and Fraunhofer SIT

Motivation

- Resource Public Key Infrastructure (RPKI) secures the interdomain routing against prefix and subprefix hijacks
- However, significant power lies with the Regional Internet Registries (RIRs)

This Work

- Distributed RPKI system that relies on threshold signatures
- Prevention rather than detection
- Ensures that any change to the RPKI objects requires a joint action by a number of RIRs, avoiding unilateral IP address takedowns
- No changes required at Relying Parties

Outline

Prefix hijacks

Russian telco hijacks internet traffic for Google, AWS, Cloudflare, and others

Rostelecom involved in BGP hijacking incident this week impacting more than 200 CDNs and cloud providers.

By Catalin Cimpanu for Zero Day | April 5, 2020 -- 21:53 GMT (22:53 BST) | Topic: Security

RPKI

RPKI [RFC 6480] is a hierarchical PKI that includes:

Routing Certificate (RC) Binds IP prefix to a public key

Route Origin Authorization (ROA) Binds the prefix to AS

- Signed by the public key associated with the RC

Route Origin Validation (ROV) Validates the origin of BGP route announcements

RPKI is a prerequisite for BGPSec [RFC 8205] that provides path validation.

Delegated and Hosted RPKI

Delegated RPKI

- Members run their own CA
- Member generates its own certificate, gets it signed by the parent CA

[1] https://ripe77.ripe.net/presentations/156-RPKI-deployment-at-scale-RIPE-1.pdf

Delegated and Hosted RPKI

Delegated RPKI

- Members run their own CA
- Member generates its own certificate, gets it signed by the parent CA

Hosted RPKI

- RIR runs the CA for the members and manages the keys and repo
- Convenient option for members as they do need to run their own CAs
- Even some large providers such as Cloudflare use hosted RPKI [1]

[1] https://ripe77.ripe.net/presentations/156-RPKI-deployment-at-scale-RIPE-1.pdf

Delegated and Hosted RPKI

Delegated RPKI

- Members run their own CA
- Member generates its own certificate, gets it signed by the parent CA

Hosted RPKI

- RIR runs the CA for the members and manages the keys and repo
- Convenient option for members as they do need to run their own CAs
- Even some large providers such as Cloudflare use hosted RPKI [1]

[1] https://ripe77.ripe.net/presentations/156-RPKI-deployment-at-scale-RIPE-1.pdf

Power imbalance

- RPKI authorities can revoke and allocations
- RPKI authorities can unilaterally takedown IP prefixes
  - Law enforcement [2] [3]
  - ASes not necessarily in the same country as the RIR (no recourse, loss of business)
- RIRs do not usually collude with each other, and often disagree with each other when it comes to their response to law enforcement agencies [4]

[2] RIPE NCC Blocks Registration in RIPE Registry Following Order from Dutch Police (2011)

[3] ICANN Tells U.S. Court That ccTLDs Are Not "Property" — Files Motion to Quash in U.S. Legal Action Aimed at Seizing Top-Level Domains (2014)

[4] M. Mueller, M. van Eeten, and B. Kuerbis. In important case, RIPE-NCC seeks legal clarity on how it responds to foreign court orders (2011)

Prior Works

- Adding transparency logs and *.dead* objects to signify consent [5]
  - Relying parties take a part of the burden
  - Detection after the fact
  - Parent manages the signing in hosted RPKI and can sign the *.dead* objects itself

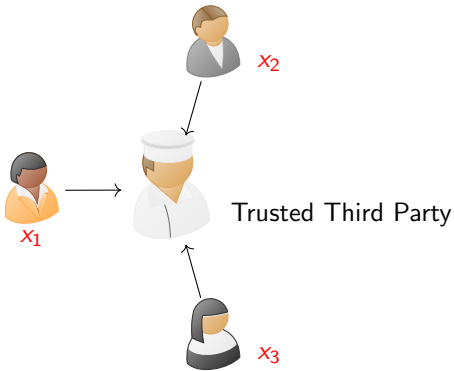
- Blockchain to replace RPKI [6]
  - Scalability
  - Deployment issues such as consensus algorithm and incentive for the nodes to run the blockchain
  - If Proof-of-Stake is used, large providers will become powerful players; another form of power imbalance

[5] Heilman, et. al. From the consent of the routed: Improving the transparency of the RPKI (SIGCOMM'14)

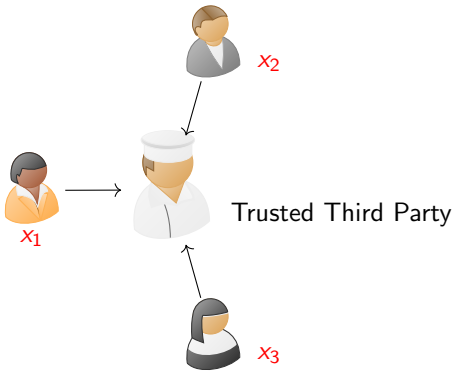
[6] Adiseshu Hari and T. V. Lakshman. The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet (HotNets'16)

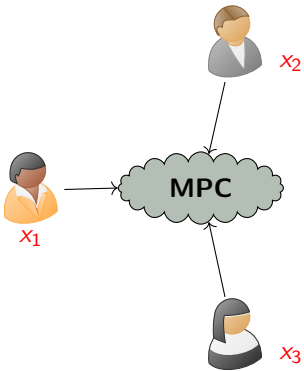
Outline

Multiparty Computation (MPC)

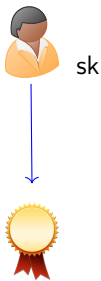


Multiparty Computation (MPC)



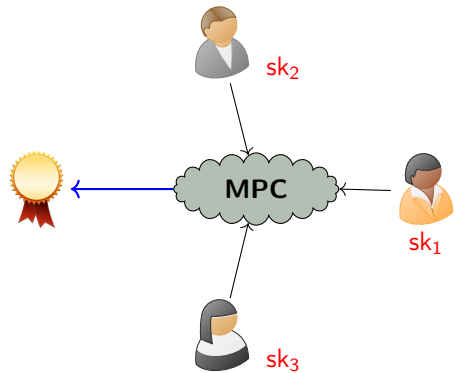


Traditional Signatures



Threshold Signatures

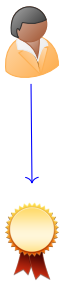
$\{sk_1, sk_2, sk_3\} \leftarrow Share(sk)$



MPC

Threshold Signatures

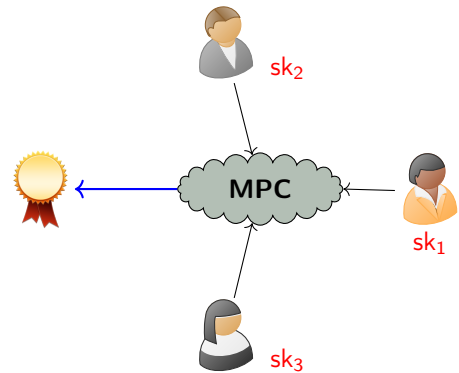
Traditional Signatures



Indistinguishable

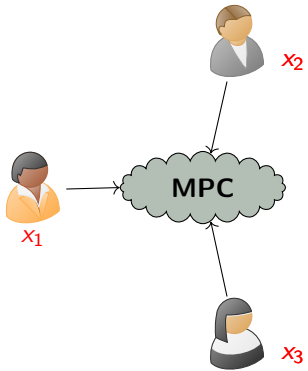
Threshold Signatures

$\{sk_1, sk_2, sk_3\} \leftarrow Share(sk)$



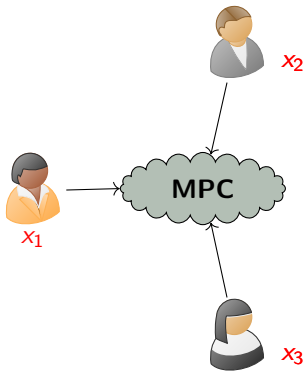
Outline

Threat model



Individual RIRs not entirely trusted

Threat model

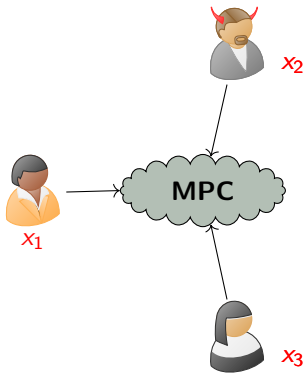


Individual RIRs not entirely trusted

Adversary power

- Passive
- Active

Threat model



Individual RIRs not entirely trusted

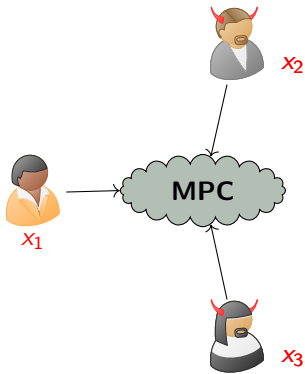
Adversary power

- Passive
- Active

How many can be corrupt?

- Minority

Threat model



Individual RIRs not entirely trusted

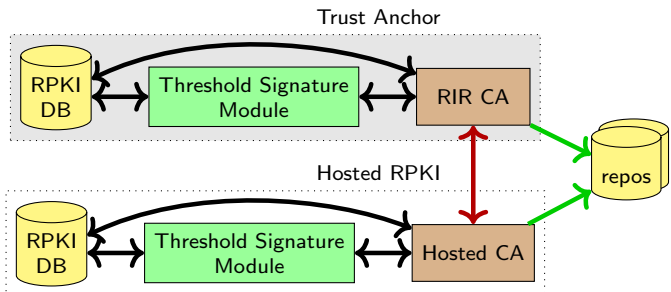
Adversary power

- Passive
- Active

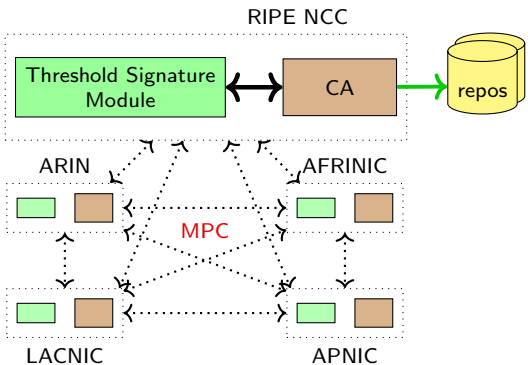
How many can be corrupt?

- Minority
- Majority

System Setup



Distributed RPKI

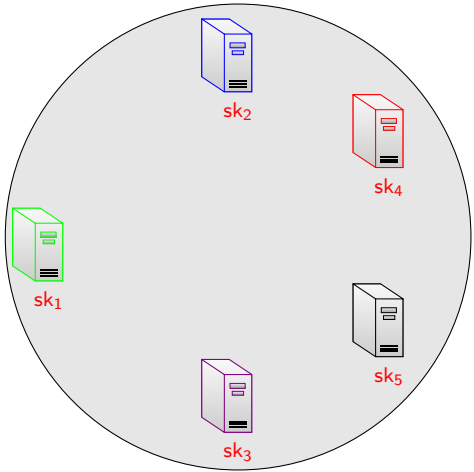


Threshold signatures for RPKI

$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3, \mathsf{sk}_4, \mathsf{sk}_5\} \leftarrow \mathit{Share}(\mathsf{sk})$

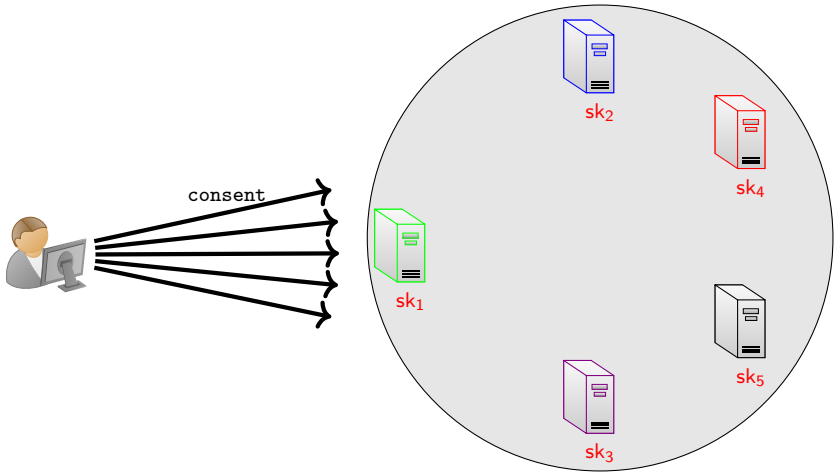
Threshold signatures for RPKI

$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3, \mathsf{sk}_4, \mathsf{sk}_5\} \leftarrow \mathit{Share}(\mathsf{sk})$



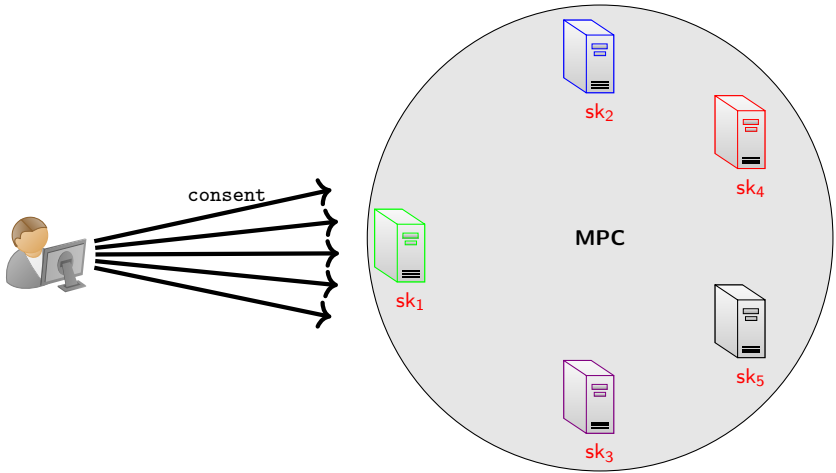
Threshold signatures for RPKI

$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3, \mathsf{sk}_4, \mathsf{sk}_5\} \leftarrow \mathit{Share}(\mathsf{sk})$



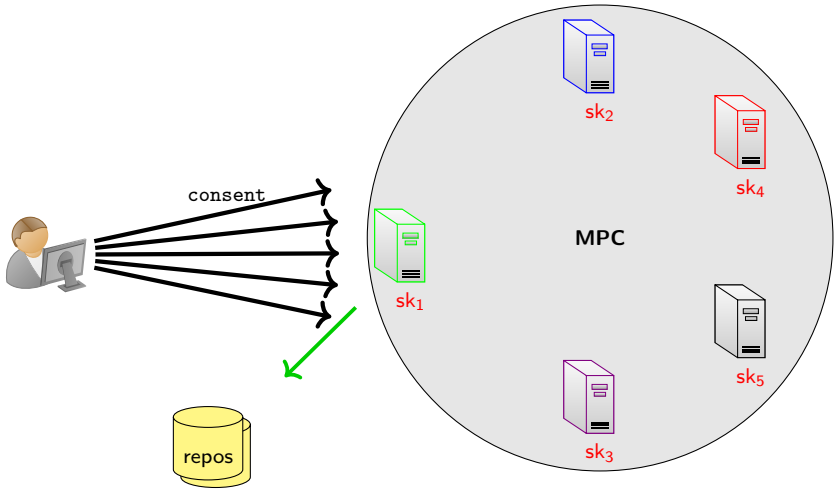
Threshold signatures for RPKI

$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3, \mathsf{sk}_4, \mathsf{sk}_5\} \leftarrow \mathit{Share}(\mathsf{sk})$



Threshold signatures for RPKI

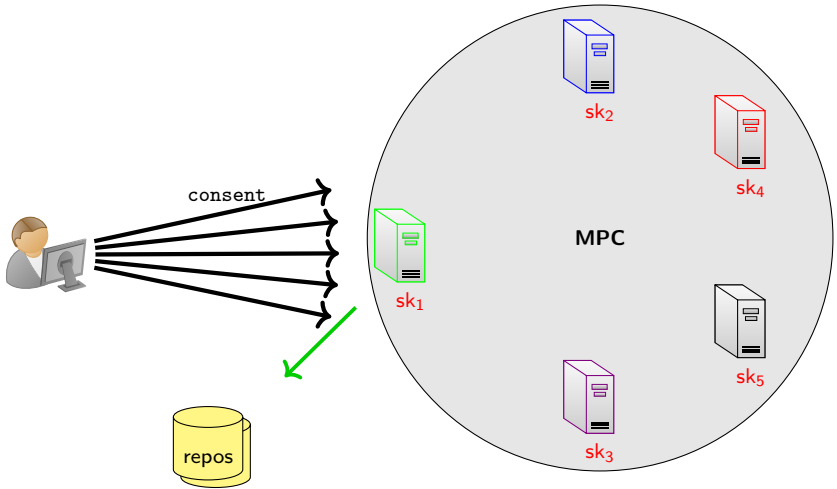
$\{\mathsf{sk}_1, \mathsf{sk}_2, \mathsf{sk}_3, \mathsf{sk}_4, \mathsf{sk}_5\} \leftarrow \mathit{Share}(\mathsf{sk})$



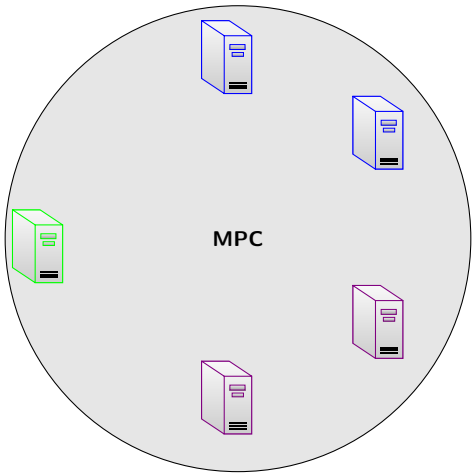
Threshold signatures for RPKI

$\{sk_1, sk_2, sk_3, sk_4, sk_5\} \leftarrow Share(sk)$

Threshold signing should not be expensive

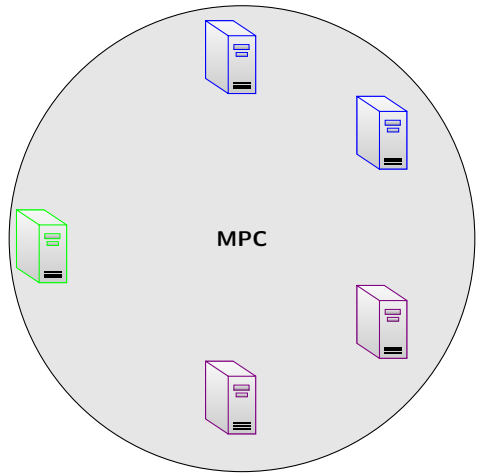


Threshold Signature in 3 phases



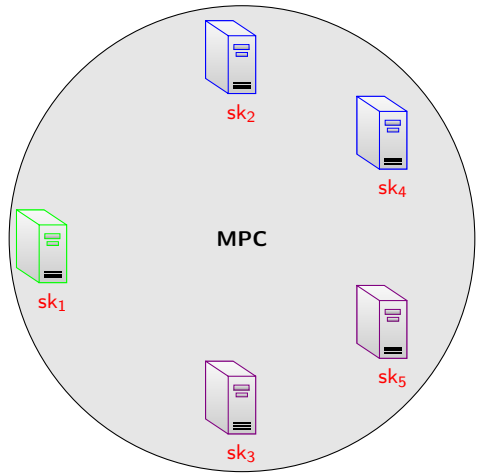
Threshold Signature in 3 phases

Preprocessing
- Member independent

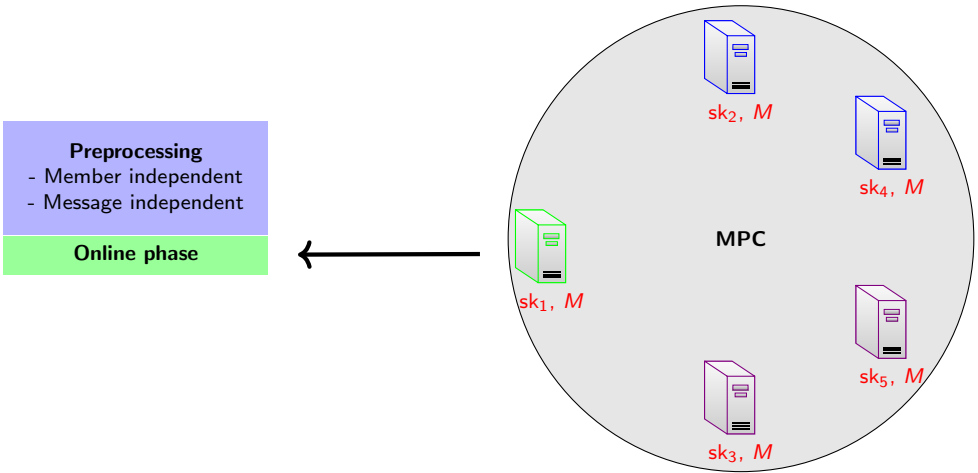


Threshold Signature in 3 phases

Preprocessing
- Member independent
- Message independent



Threshold Signature in 3 phases



Deployment Scenarios

- Two-layered
  - Is compatible with delegated RPKI
  - Upper layer generates a distributed TA to the five RIRs
  - Distributed key generation
  - All RIRs have the same subjectPublicKeyInfo in their TAL
  - Lower layer uses the threshold signing module for the Hosted CAs
  - Generates signed objects
  - Not entirely immune to state coercion
- Flat
  - Combines RIR CA and hosted CA
  - Replaces the hierarchical RPKI with a flat architecture
  - Not compatible with delegated RPKI

Evaluations

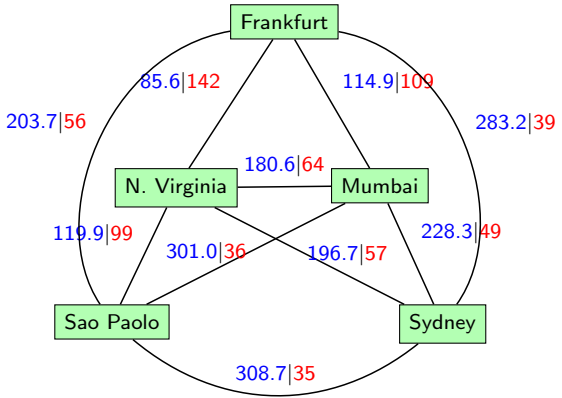


Figure: Latency in milliseconds|Bandwidth in Mbits/s between regions

Evaluations

Majority \ Adversary power	Passive	Active
Honest	Shamir	Mal. Shamir
Dishonest	Semi. OT	MASCOT

Table: Four MPC protocols

	LAN		WAN	
	Preprocessing	Online	Preprocessing	Online
MASCOT	209	529	20	0.95
Semi OT	1042	662	111	2.05
Mal. Shamir	699	714	91	3.53
Shamir	1020	769	265	3.54

Table: Breakdown of throughput for preprocessing (tuples/sec) and online phases (signatures/sec)

ROAs

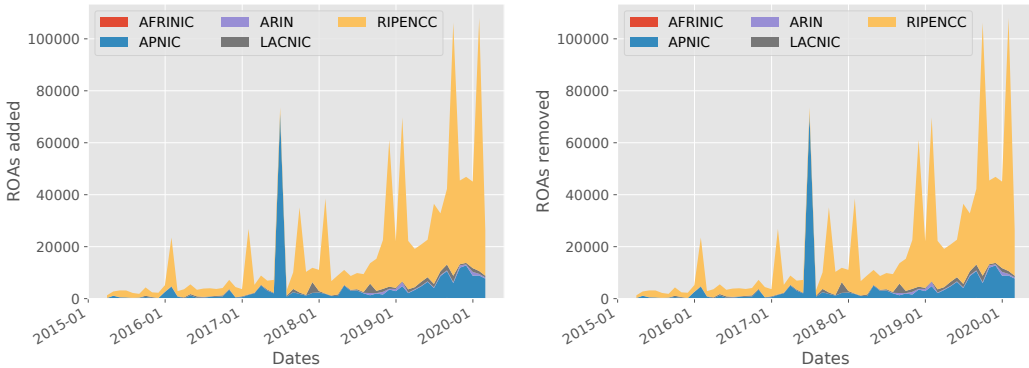


Figure: Number of ROAs added and removed from March 2015 to February 2020

Evaluations

In the WAN setting,

- MASCOT: 0.95 signatures/sec or 82080 signatures/day
- Shamir: 3.53 signatures/sec or 304992 signatures/day
- Even our slowest protocol is able to satisfy the requirements on an average day.
- Our other protocols are able to generate enough signatures even on peak days

Summary of our work

- Distributed RPKI with a stronger threat model
- Using threshold signatures in preprocessing model
- No changes at Relying Parties
- Technical solution that requires legal and policy barriers to be addressed to make the work truly practical

kris.shrishak@sit.tu-darmstadt.de