AccuRevoke: Enhancing Certificate Revocation with Distributed Cryptographic Accumulators

Munshi Rejwan Ala Muid

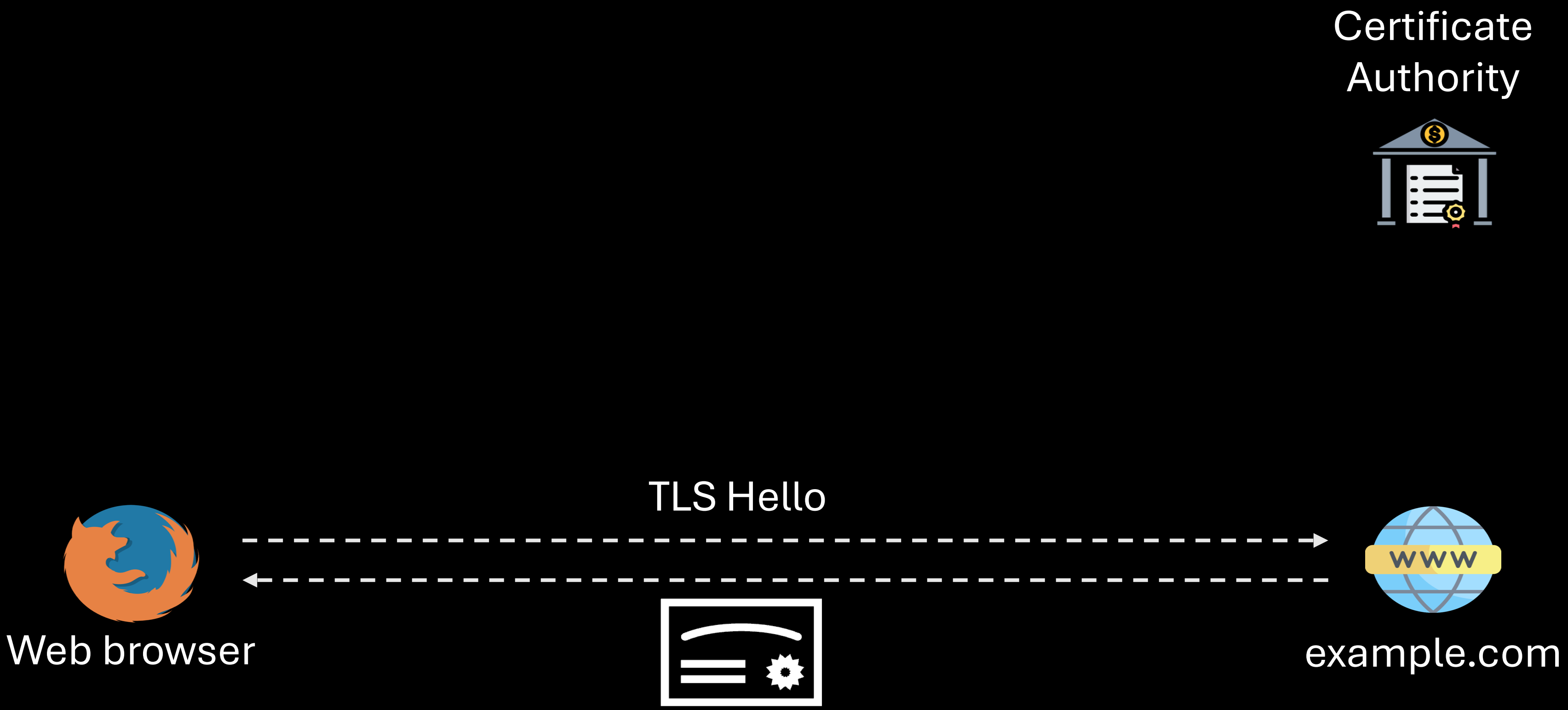
Taejoong Chung

Thang Hoang

VIRGINIA TECH

{munshira, tijay, thanghoang}@vt.edu

TLS Overview



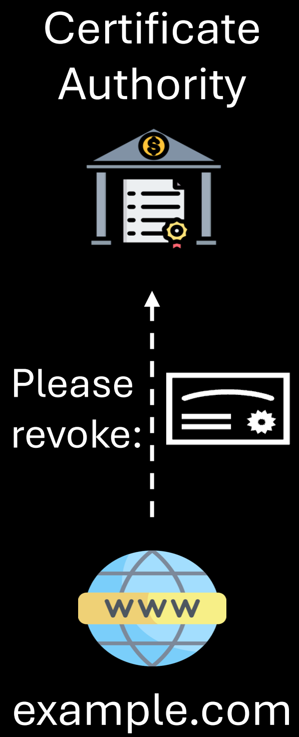
Certificate Authority

TLS Hello

Web browser

example.com

Revocation Request

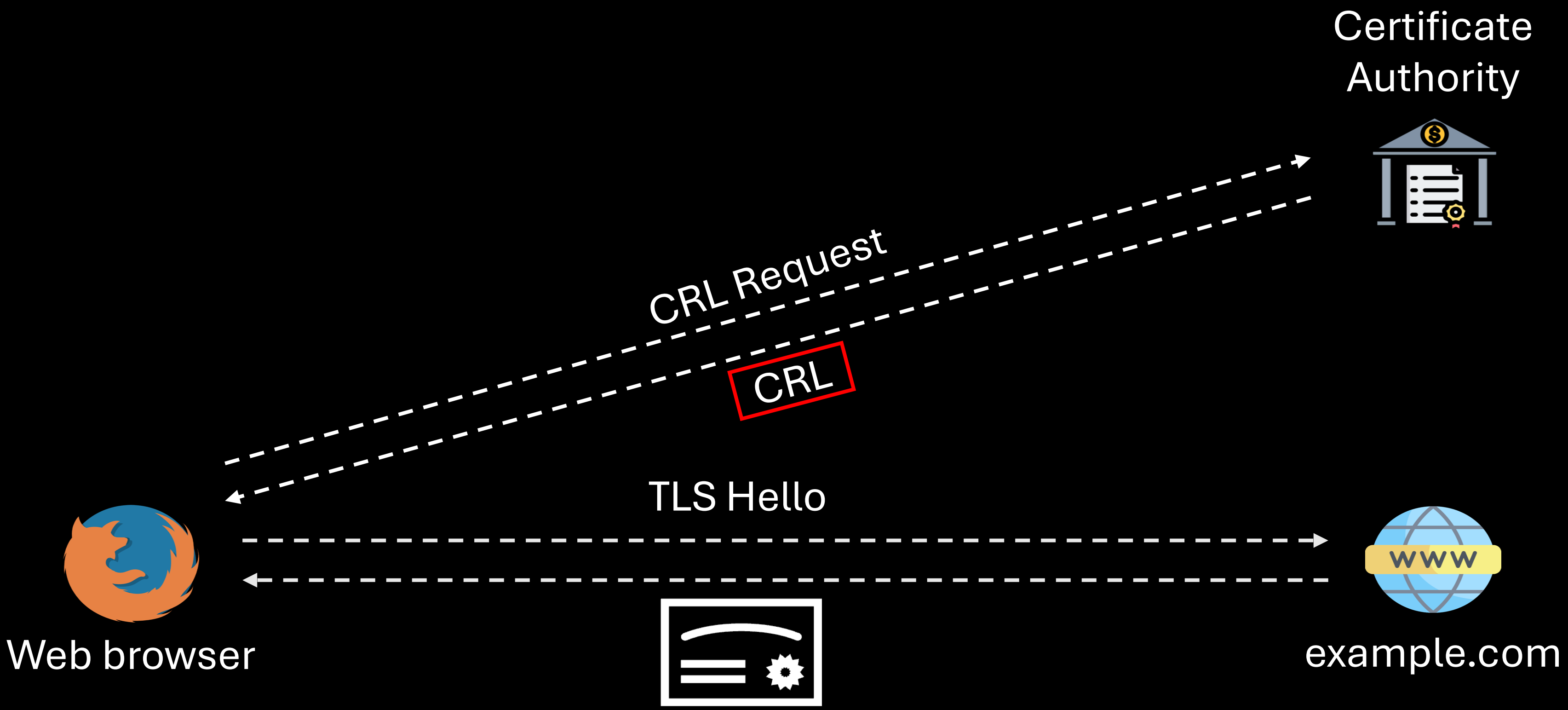


Certificate Authority

Please revoke:

example.com

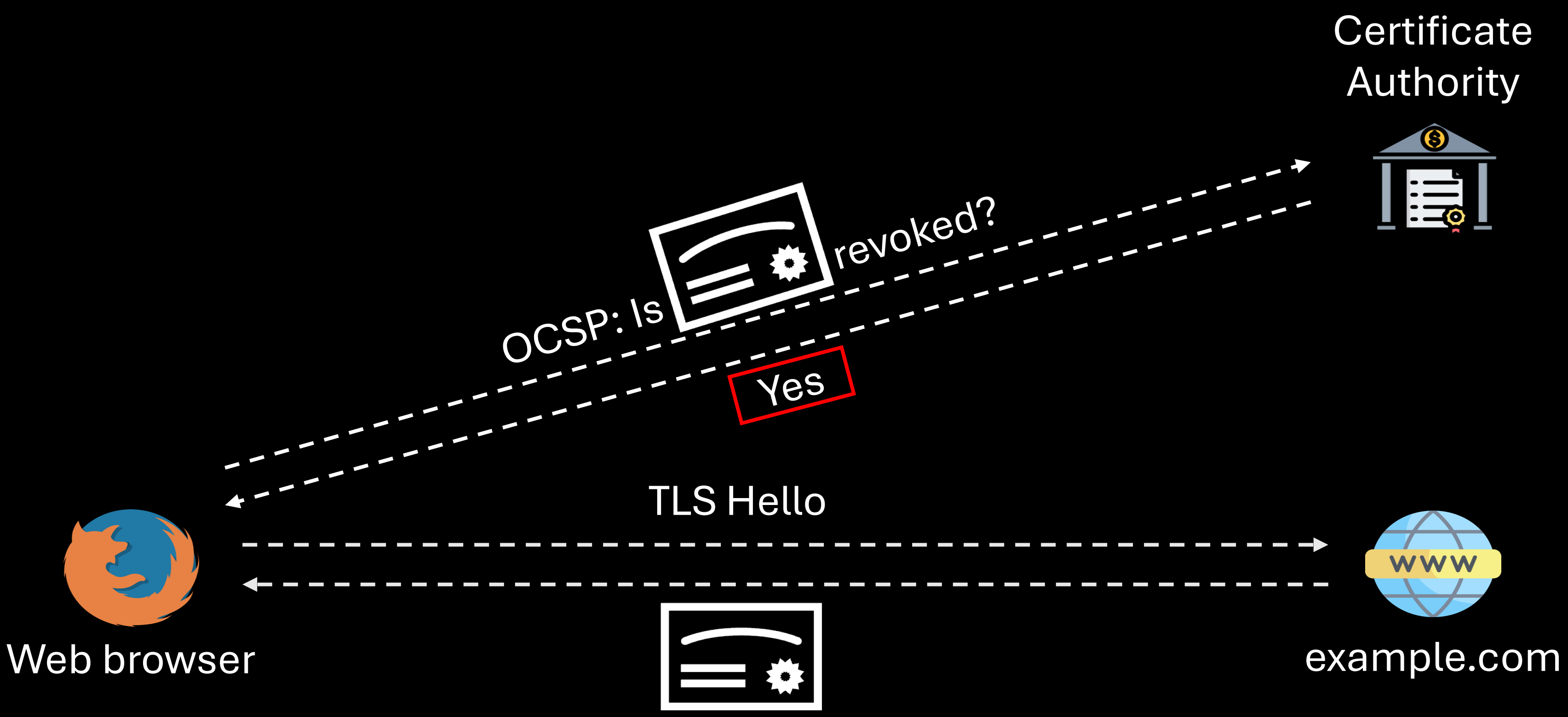
Certificate Revocation List



CRL request for every TLS handshake is untenable

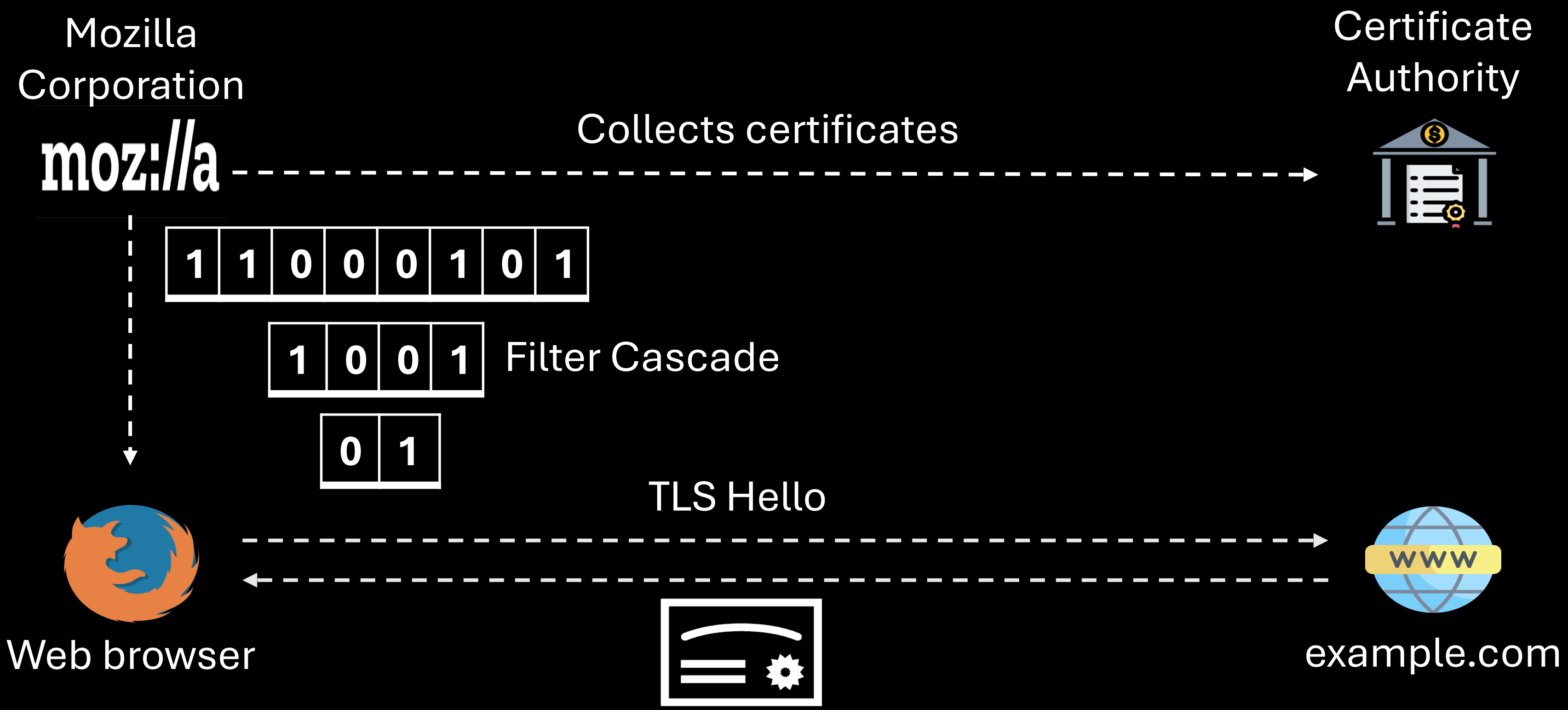
The list can be very large! 76 MB for Apple.

Online Certificate Status Protocol



- **CA overloaded by OCSP**
- **CA sees client visits**

CRLite



- **Clients rarely audit — Trust Assumed**
- **Pushing all revocations = Inefficient**
- **Daily updates miss midday revocations**

CDNs in Certificate Revocation

- Many CAs rely on CDNs (Content Delivery Networks) like Akamai and Cloudflare to distribute CRLs and serve OCSP responses.

Traditional CDN Role

Distributes CRLs and
OCSP from CA origin
Server

Revocation Goals vs. Existing Solutions

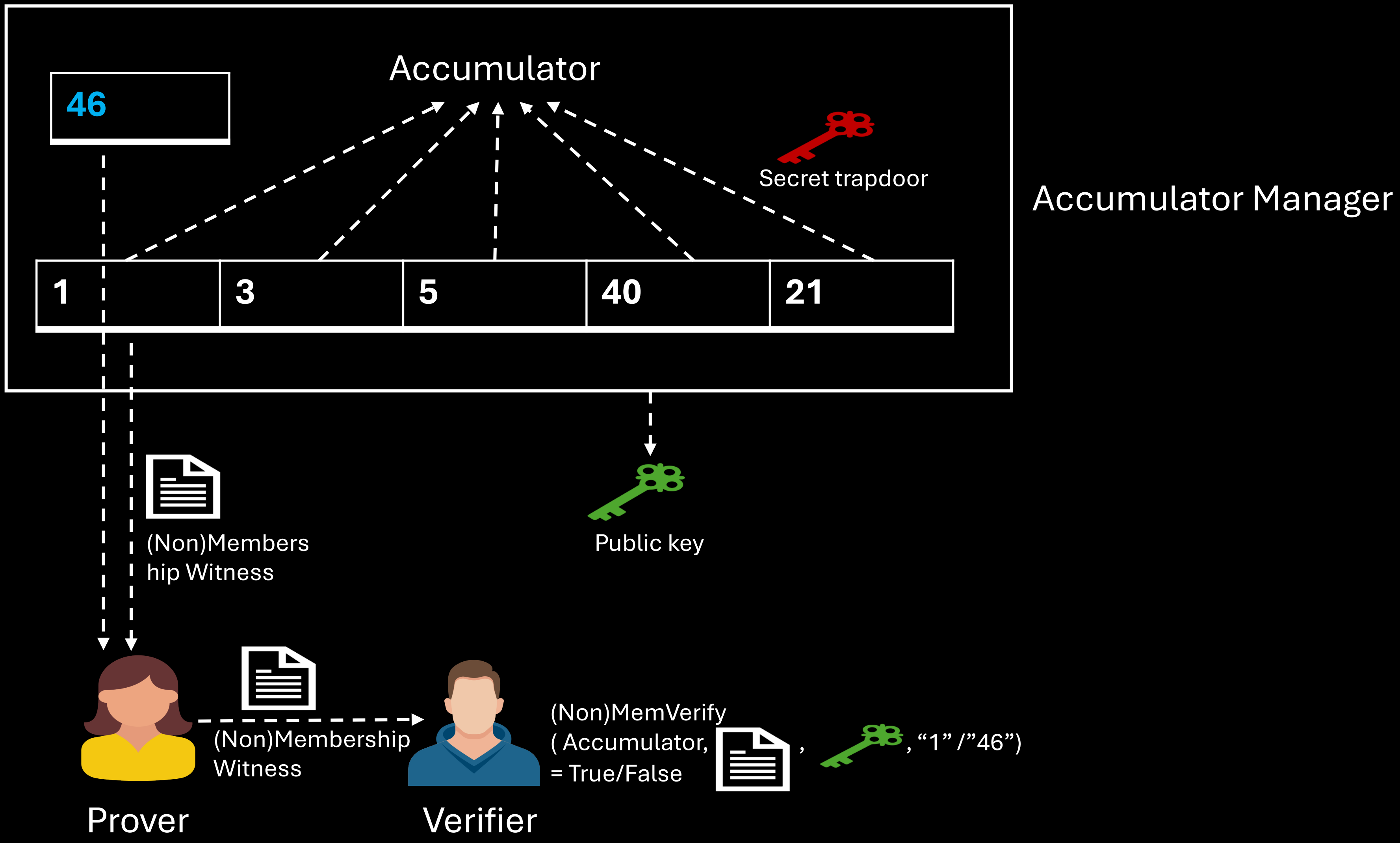
Scheme	All Revocations Covered	Latest Revocation Information	Low bandwidth cost and latency	Soft-failure Model	Privacy	No Overfetching	Auditable	Easy to Deploy
CRL	✅	✅	❌	❌	✅	❌	❌	✅
CRLite	✅	▲	✅	❌	✅	❌	▲	✅
OCSP	✅	✅	▲	✅	❌	✅	❌	✅

✅ => Achieved ▲ => Partially achieved/ Trade-off ❌ => Not achieved

AccuRevoke!

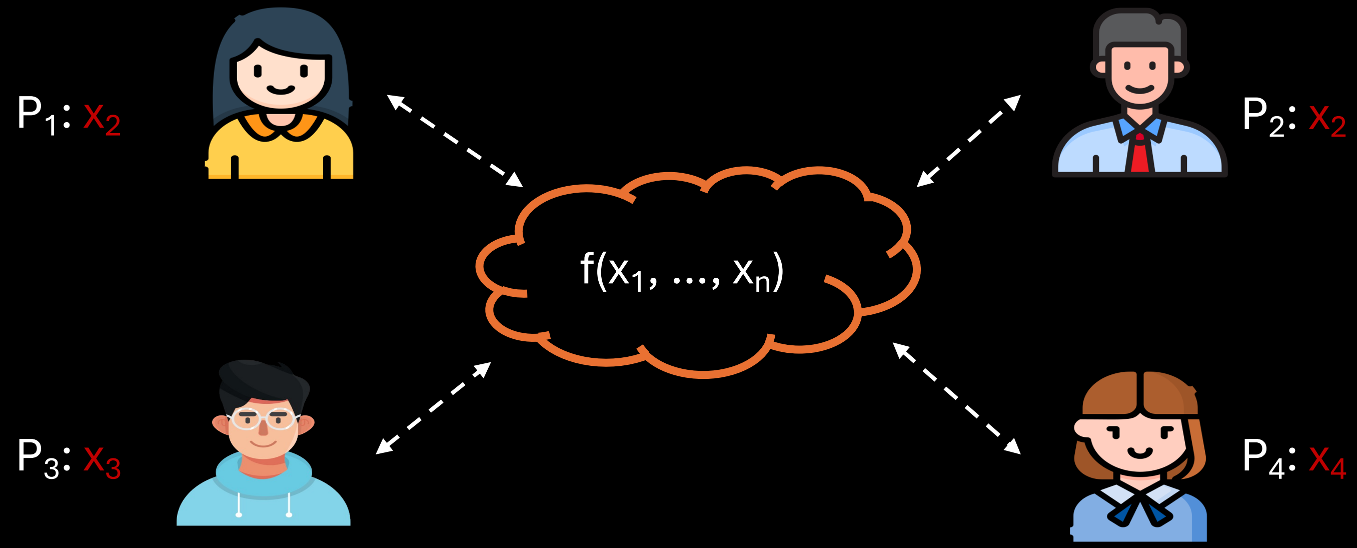
Dynamic Universal Accumulator

- **Concise representation** of a set.
- Provide **membership or non-membership proofs** for elements.
- Enable **efficient verification** of membership or non-membership using proofs.
- Supports addition and deletion.



Secure Multiparty Computation

- Parties jointly compute a function on their private inputs without revealing them.



AccuRevoke: System Model

Edge Compute Providers

ECP_1

ECP_3

ECP_2

- Third party servers
- Participate in SMPC to generate witness for a revoked or non-revoked certificate.
- Sends the witness of a certificate upon request from the client.

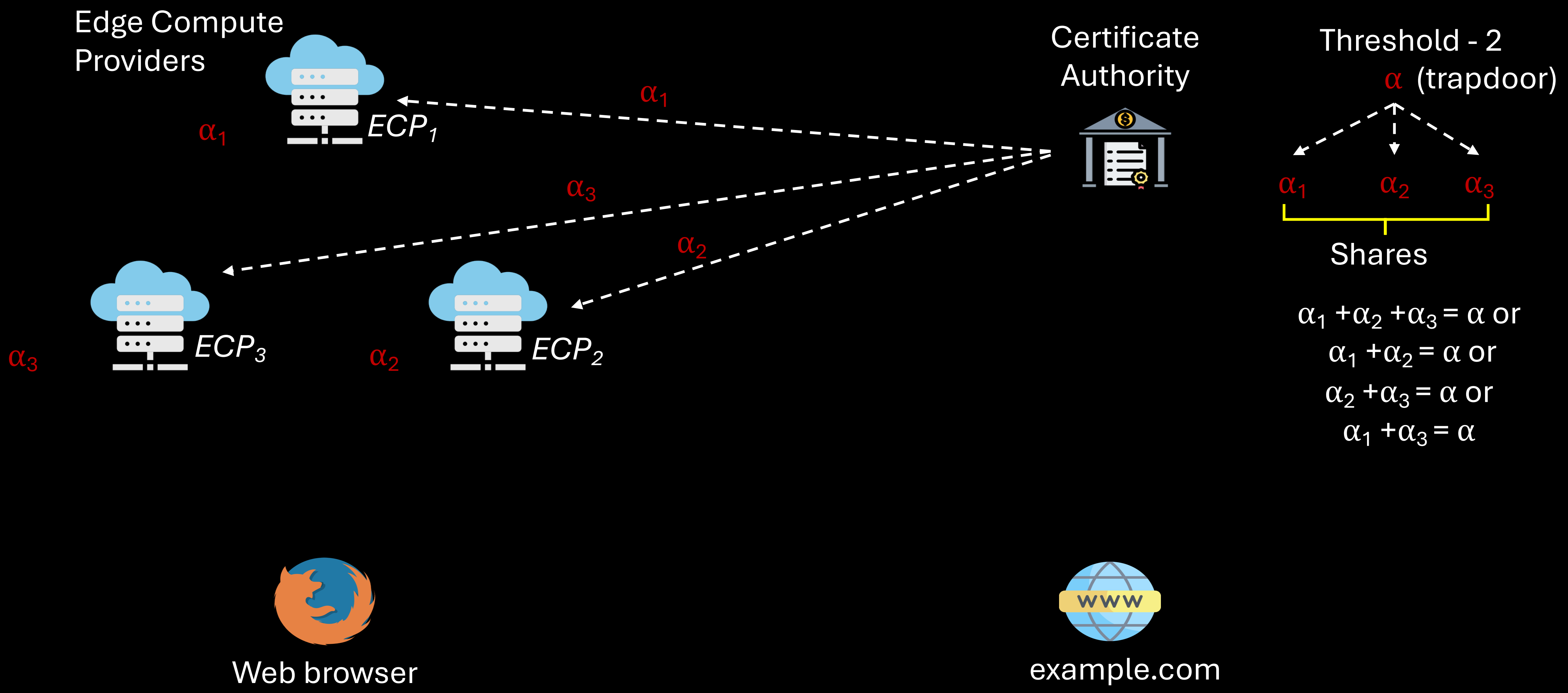
Certificate Authority

- Main source of trust
- Creates accumulator from the list of revoked certificates.
- Delegates trust to multiple third parties.

Web browser

example.com

AccuRevoke: Creating two Layers of Trust



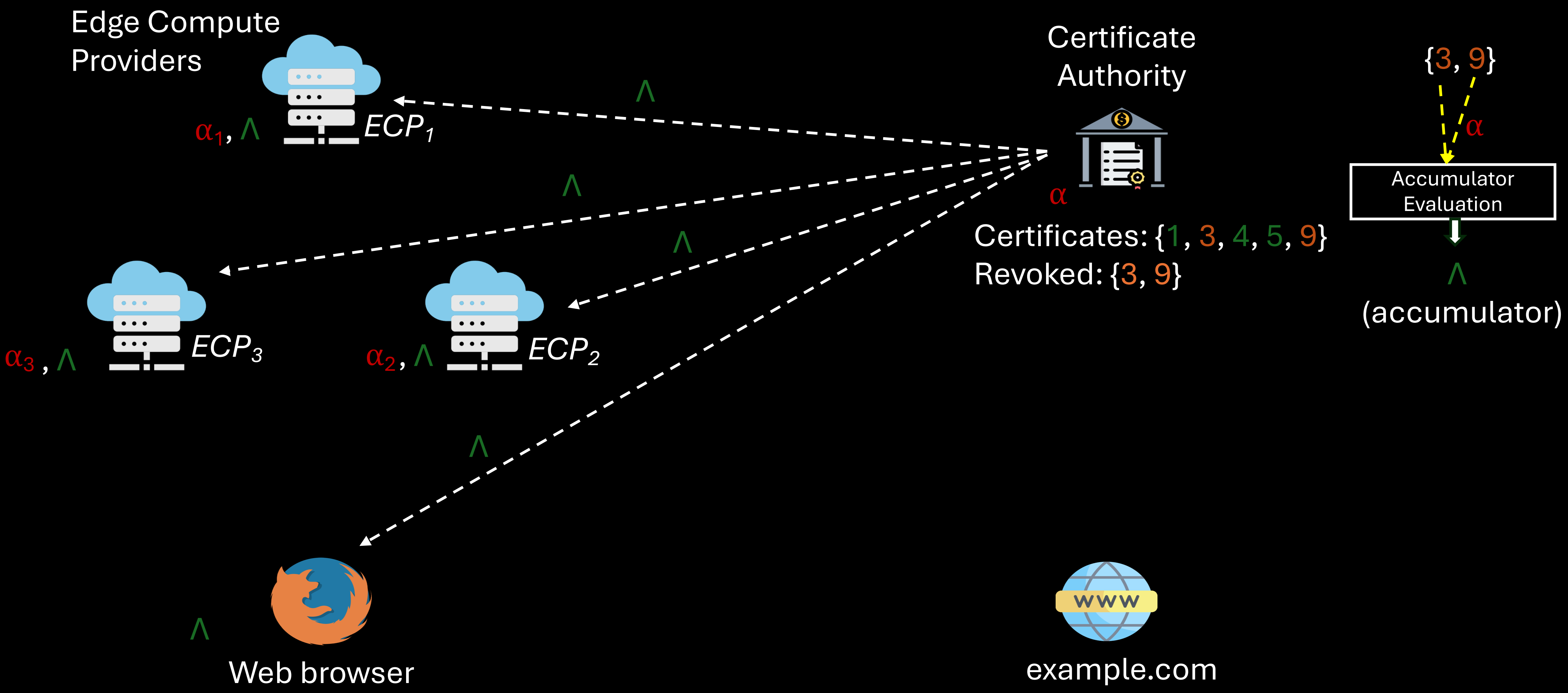
$\alpha_1 + \alpha_2 + \alpha_3 = \alpha$ or

$\alpha_1 + \alpha_2 = \alpha$ or

$\alpha_2 + \alpha_3 = \alpha$ or

$\alpha_1 + \alpha_3 = \alpha$

Accumulator Generation and Dissemination



Edge Compute Providers

α_1, Λ ECP_1

α_3 , Λ ECP_3

α_2, Λ ECP_2

Λ

Λ

Λ

Λ

Λ

Web browser

Certificate Authority

α

Certificates: {1, 3, 4, 5, 9}

Revoked: {3, 9}

{3, 9}

α

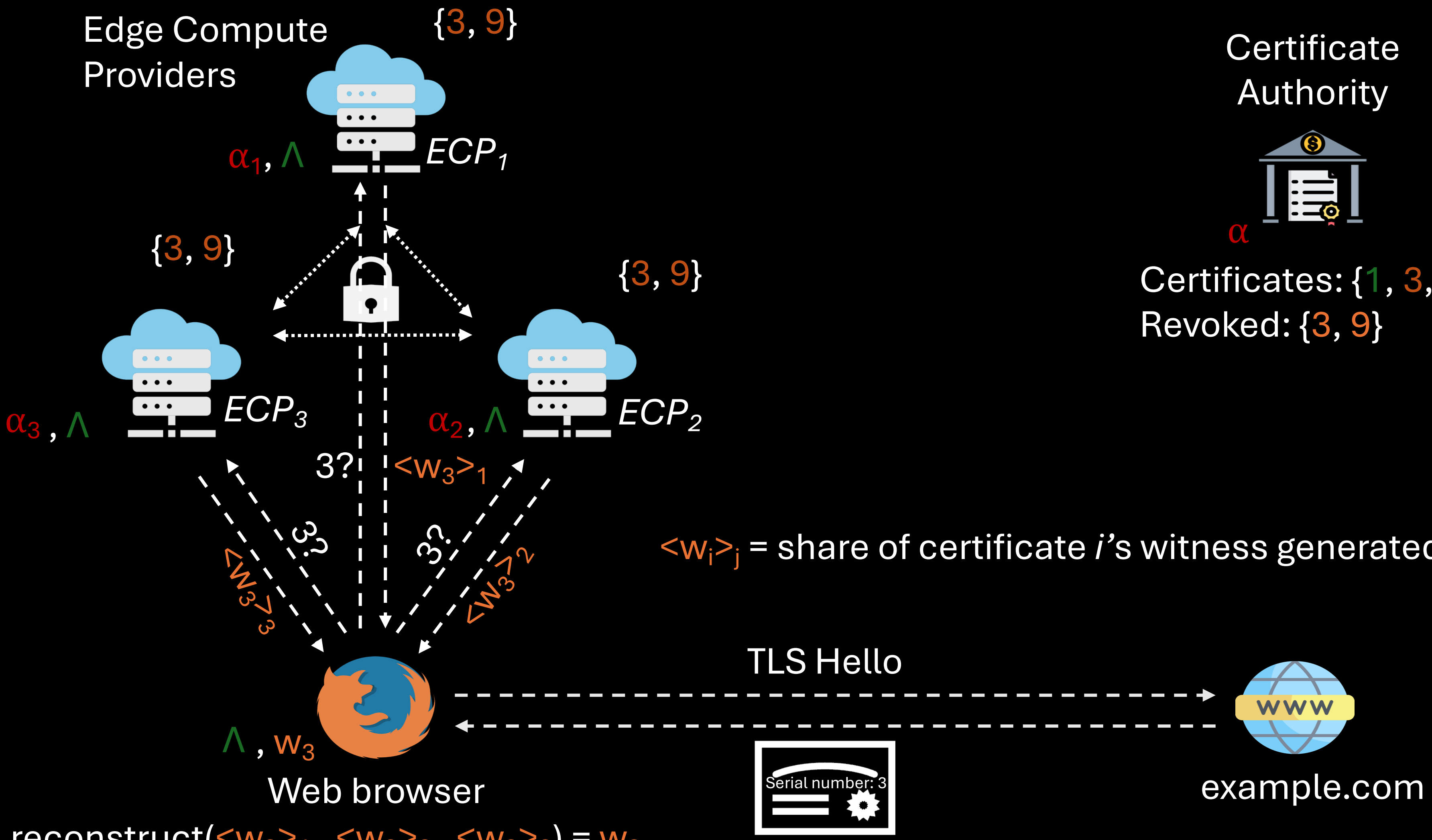
Accumulator Evaluation

Λ

(accumulator)

example.com

Witness Generation– Client-side Reconstruction



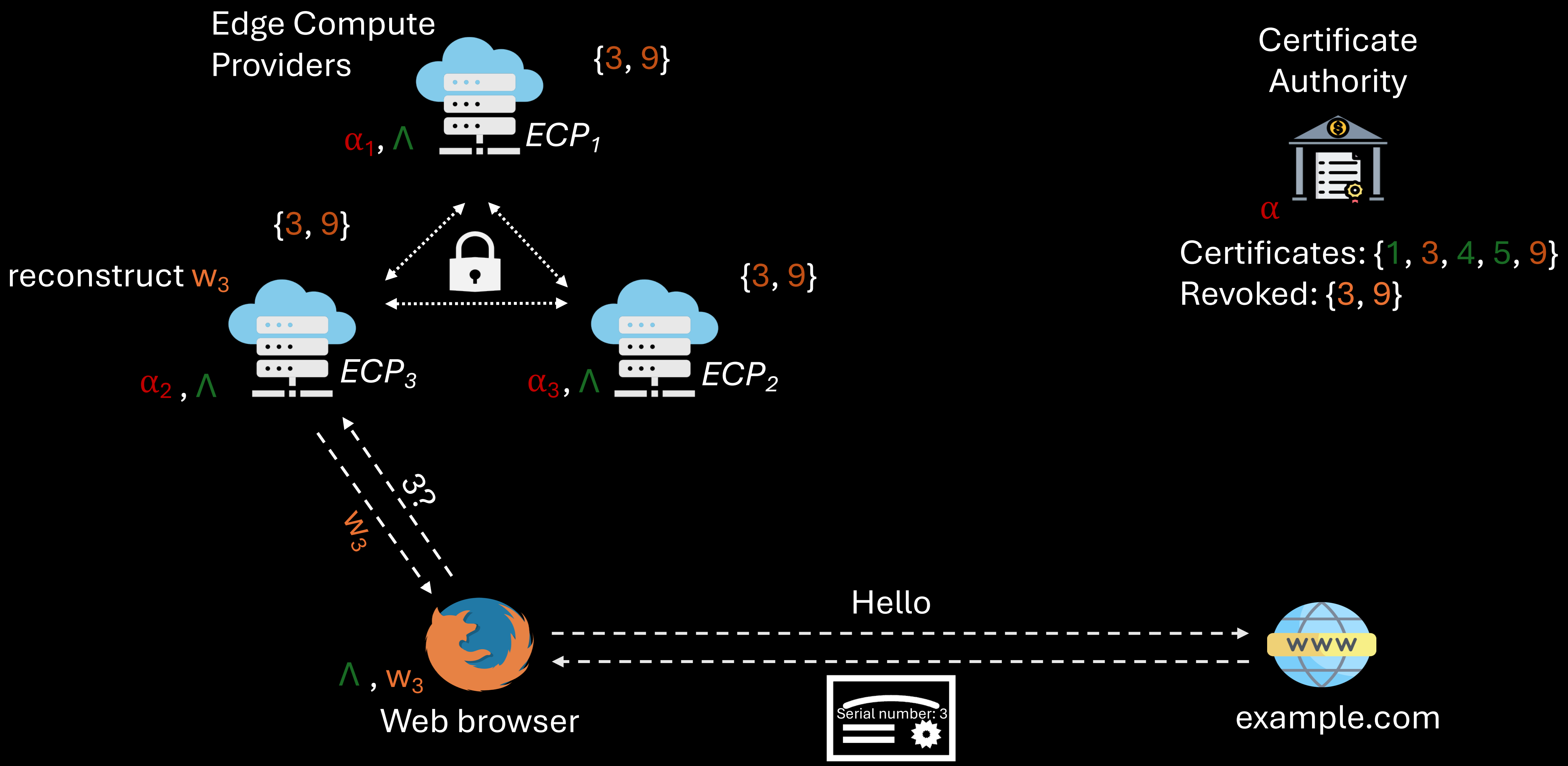
Certificates: {1, 3, 4, 5, 9}
Revoked: {3, 9}

$<w_i>_j$ = share of certificate *i*’s witness generated by ECP_j

reconstruct($<w_3>_1$, $<w_3>_2$, $<w_3>_3$) = w_3

verify(Λ, w_3,) = true/false

Witness Generation– Single ECP Reconstruction



Edge Compute Providers

$\{3, 9\}$

α_1, Λ ECP_1

$\{3, 9\}$

reconstruct w_3

α_2, Λ ECP_3

$\{3, 9\}$

α_3, Λ ECP_2

3?

w_3

Λ, w_3

Web browser

Hello

Serial number: 3

example.com

Certificate Authority

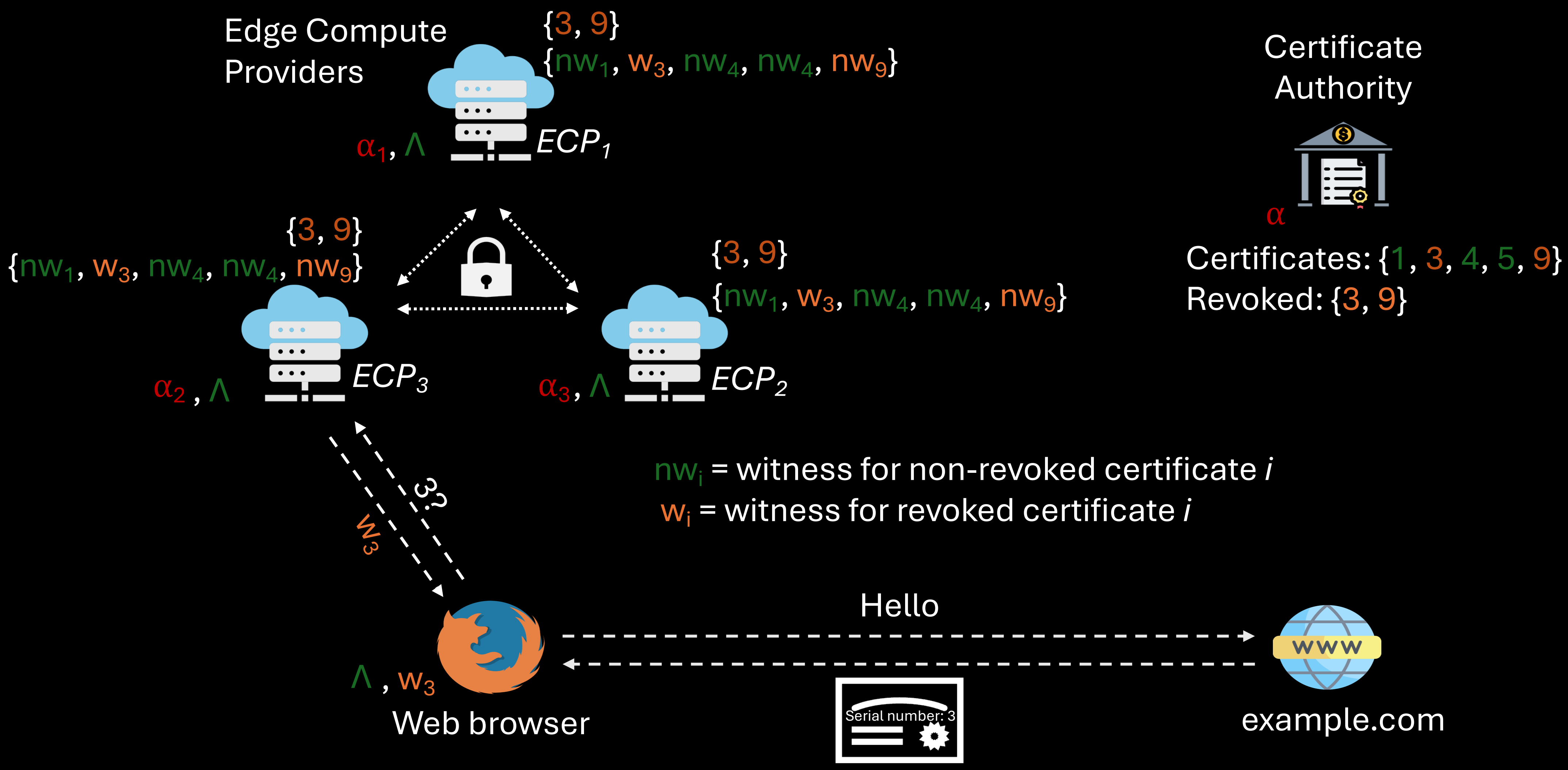
α

Certificates: {1, 3, 4, 5, 9}

Revoked: {3, 9}

verify(Λ, w_3, ▭) = true/false

Witness Generation– Multiple ECPs Reconstruction

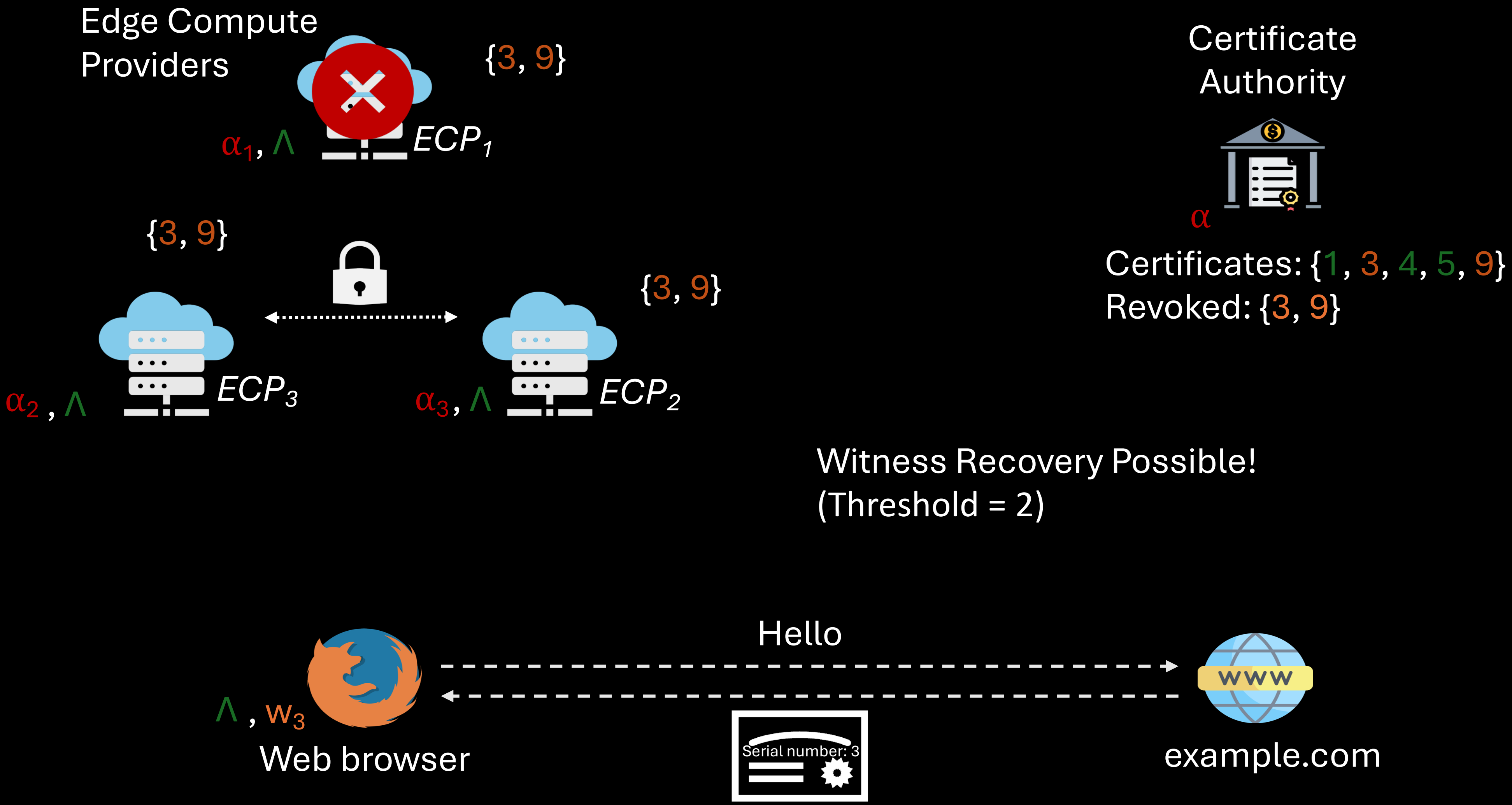


Certificates: {1, 3, 4, 5, 9}
Revoked: {3, 9}

nw_i = witness for non-revoked certificate *i*
w_i = witness for revoked certificate *i*

verify(Λ, w_3, Serial number: 3) = true/false

AccuRevoke: Robustness



Edge Compute Providers

{3, 9}

α_1, Λ ECP_1

{3, 9}

{3, 9}

α_2 , Λ ECP_3

α_3, Λ ECP_2

Certificate Authority

α

Certificates: {1, 3, 4, 5, 9}

Revoked: {3, 9}

Witness Recovery Possible!
(Threshold = 2)

Hello

Λ , w_3

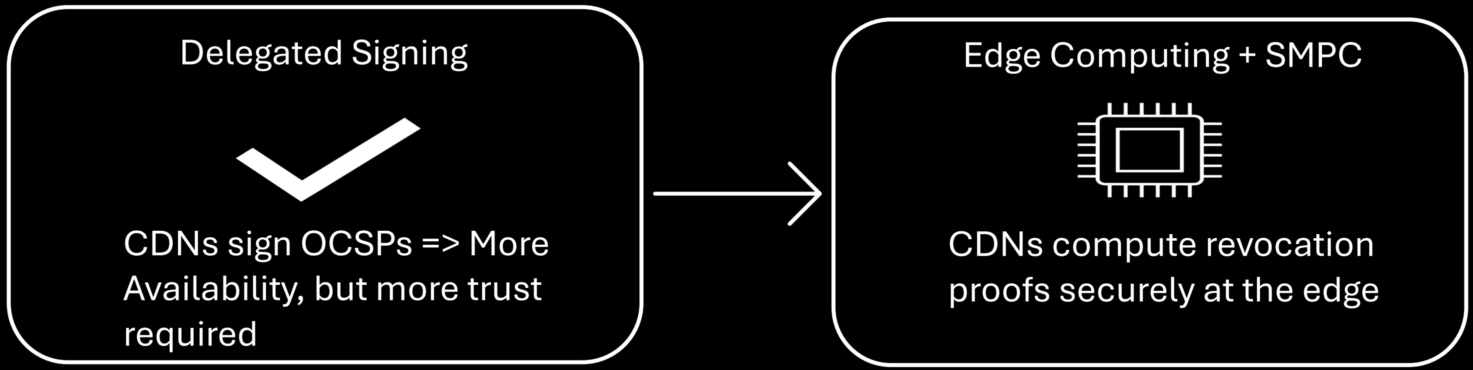
Web browser

Serial number: 3

example.com

ECPs in Certificate Revocation

- Challenges in Using CDNs
  - Delegated signing boosts availability but expands trust to CDNs.
- New Direction in CDN
  - CDNs now offer edge computing (e.g., Cloudflare Workers) and we call these ECPs.
  - Enables fast, local revocation checks near clients.



Delegated Signing

CDNs sign OCSPs => More Availability, but more trust required

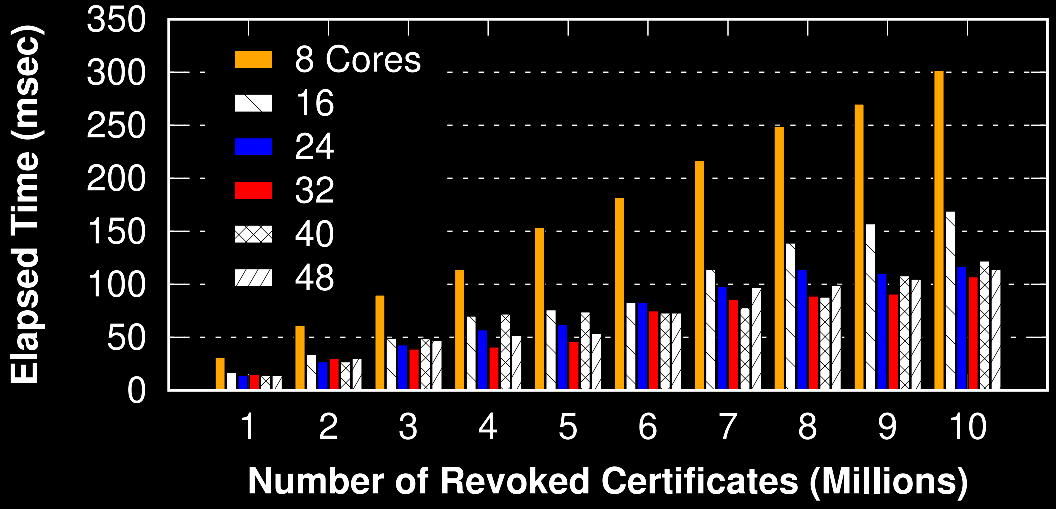
Edge Computing + SMPC

CDNs compute revocation proofs securely at the edge

Experimental Results

Accumulator Evaluation by CA:

- One-time cost
- Size – 21 bytes (Constant!)
- Parallel processing helps!



Accumulator Update by CA:

- Deletion/ Addition – 0.47 ms on average

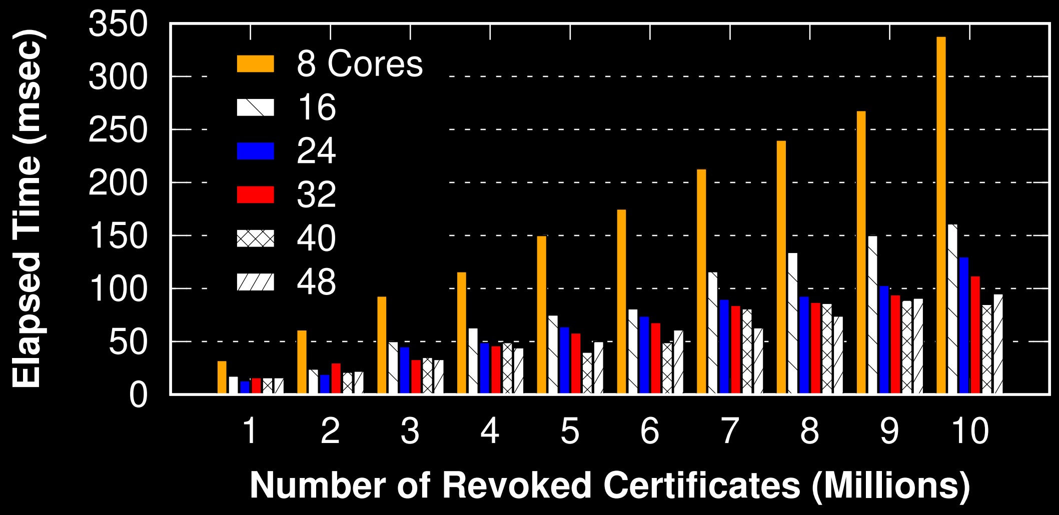
Experimental Results

Witness for a revoked certificate:

- Size – 21 bytes!
- Time – 0.46 ms on average

Witness for a non-revoked certificate:

- Size – 61 bytes!

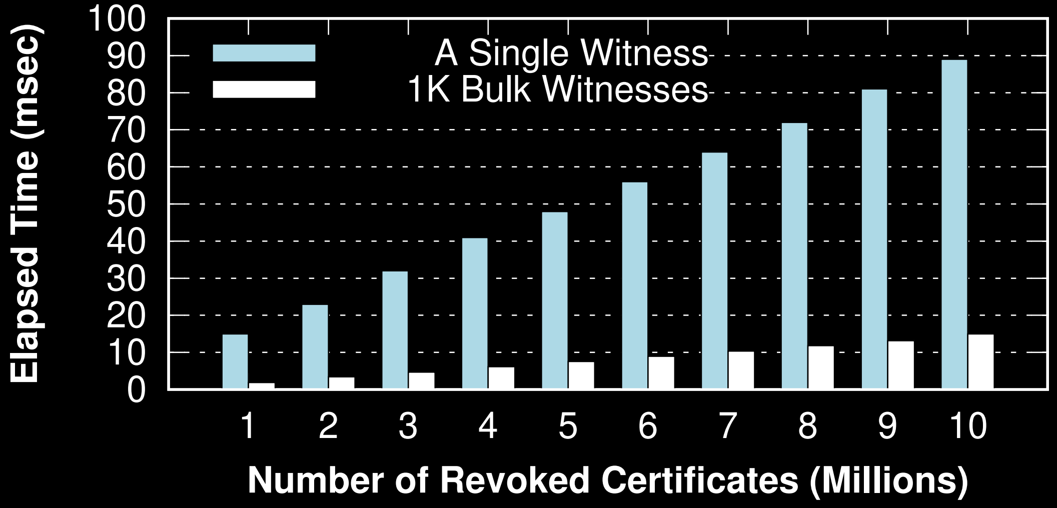


🔁 High cost for one non-revoked cert?
⚡ GPU acceleration possible?
☁️ Cloudflare offers GPU services!

Experimental Results

Witness for a non-revoked certificate on GPU:

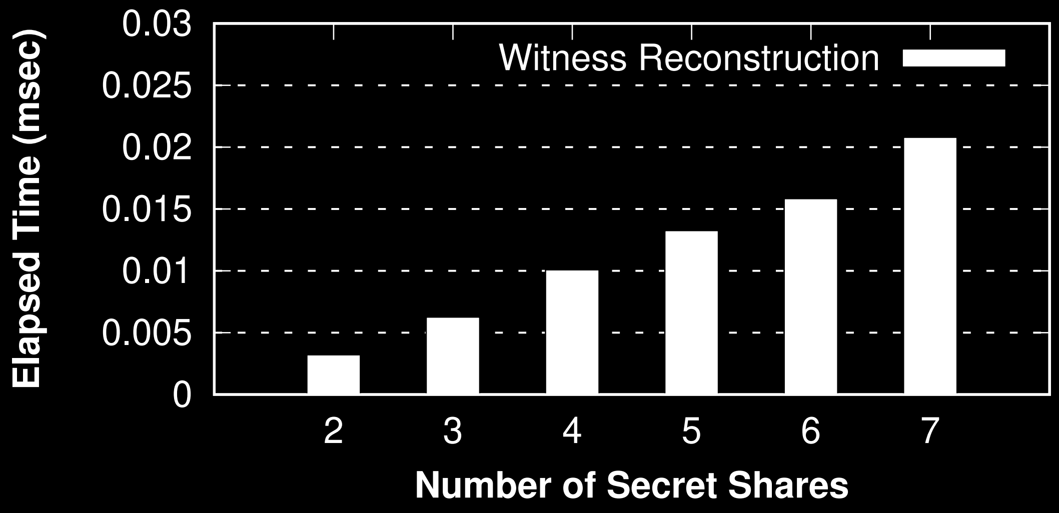
- Single non-membership witness - 15 ms.
- Single non-membership witness with amortization – 1.8 ms.
- 8.9-fold speedup!



Experimental Results

Witness Reconstruction:

- By one ECP or multiple ECPs or client
- Depends on the threshold value in Shamir set by CA



Did we keep our promise?

Desired Properties	Achieved?
All Revocations Covered	✅
Low Bandwidth Cost	✅ (21 or 61 B per request)
Privacy	✅ (if used with DNS due to shorter proof size)
Auditability	✅
Soft-failure model	✅
Easy to deploy	✅
Latest Revocation Information	✅
No Overfetching	✅

Comparison with Other Revocation Strategies

Scheme	Revocation Covered	Pull Model	Bandwidth Cost	Bytes downloaded	Delay	Privacy Dead Origin	Works with Auditable	Authenticity Model	Failure
CRL	All	❌	173 KB per CRL	31.7 MB	378.7 sec	●	●	●	Hard-fail
CRLite	All	❌	580 KB per day	0.58 MB	6.4 sec	●	●	●	Hard-fail
OCSP	All	●	1.3 KB per request	1.30 MB	74.8 sec	▲	❌	▲	Soft-fail
AccuRevoke	All	●	21 or 61 B per request	0.06 MB	86.9 sec	▲	●	●	Soft-fail

● => Achieved

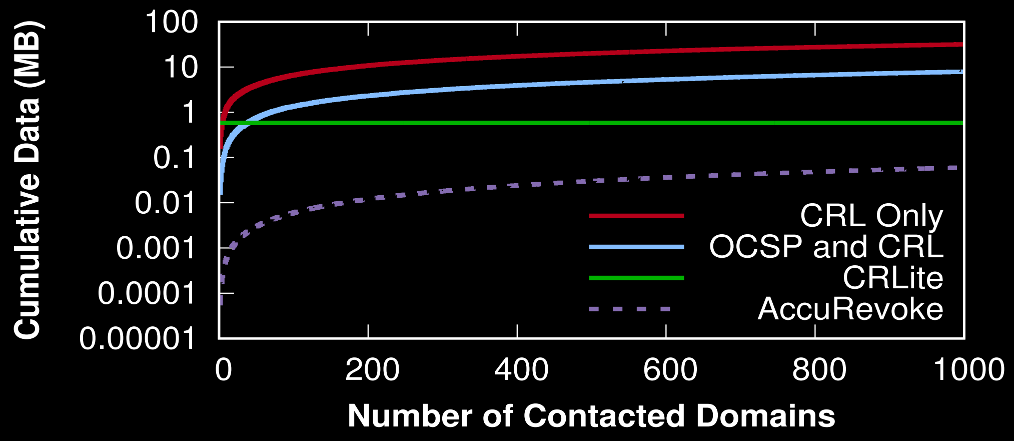
▲ => Partially achieved/ Trade-off

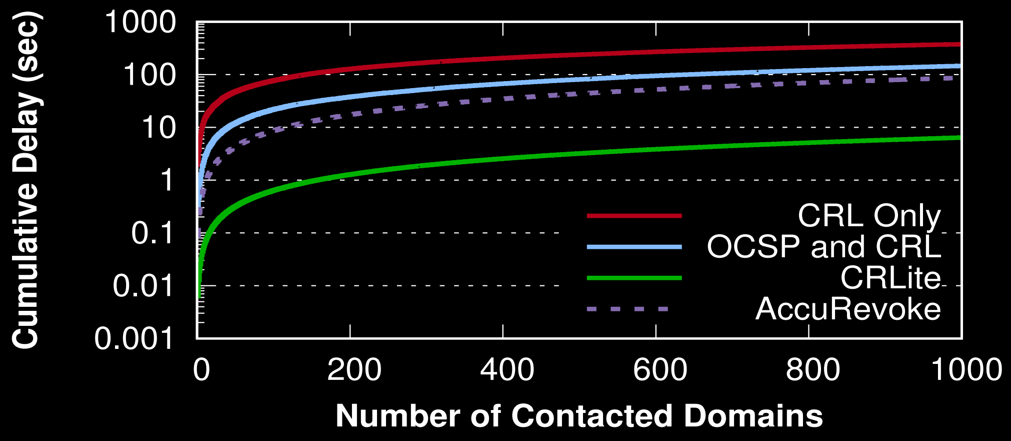
❌ => Not achieved

Client Simulation: How Does AccuRevoke perform?

Client Simulation Summary

- Simulated client behavior across 1,000 domains
- AccuRevoke minimizes total data downloaded
- Slightly higher delay than CRLite, but CRLite's limitations give AccuRevoke the advantage





Thank you!

Contact: munshira@vt.edu
Source code available at: *https://accurevoke.netsecurelab.org*