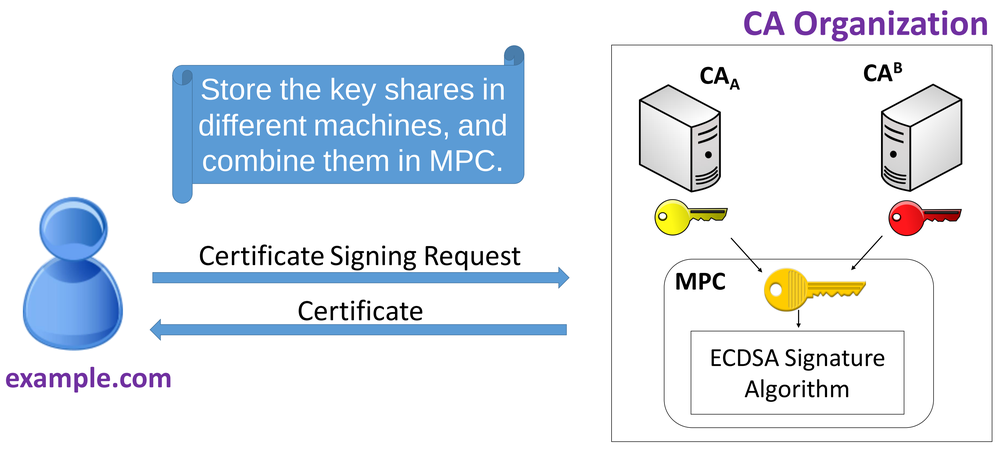
# Decentralized Certificate Authorities

Hannah Li+, Bargav Jayaraman+ and David Evans
*University of Virginia*
oblivc.org/dca

## Overview

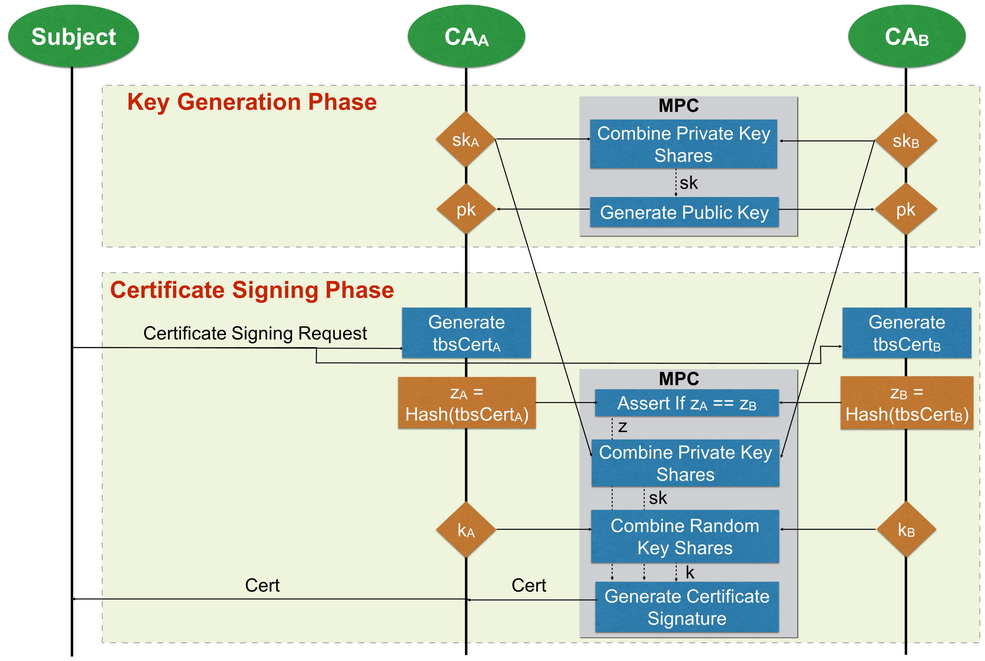
The security of TLS depends on trust in certificate authorities, and that trust stems from their ability to protect and control the use of a private signing key. The compromise of a CA private key represents a single point-of-failure that could have disastrous consequences, so CAs go to great lengths to attempt to protect and control the use of their private keys. Nevertheless, keys are sometimes exposed and misused accidentally or intentionally by insiders.

We demonstrate multi-party key signing with MPC.



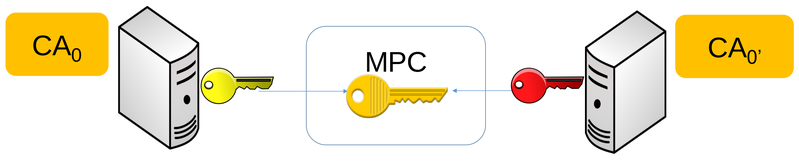

## Implementation

We use the Obliv-C framework that includes the latest enhancements to Yao's garbled circuits protocol. Apart from the Yao's protocol for garbled circuits that is secure against semi-honest adversaries, Obliv-C also implements the dual execution protocol to provide security against active adversaries.

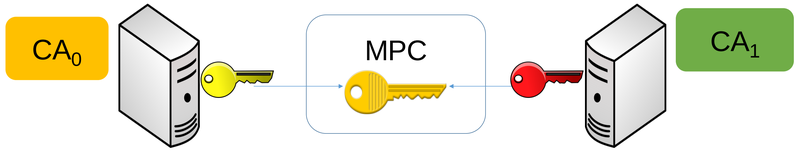



## Application Scenarios

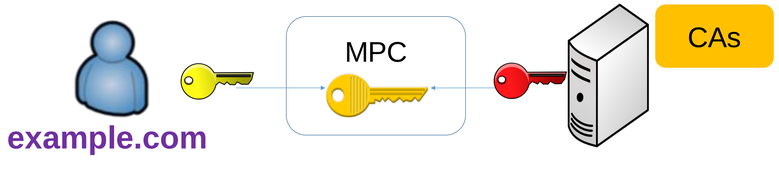
1. A single CA wants to protect its signing key




2. Two independent CAs jointly sign certificates




3. Subject is also involved in its certificate signing




## Experimental Results

We have conducted experiments using Amazon AWS EC2 nodes to jointly sign a certificate using ECDSA on curve *secp192k1* using Yao's protocol and dual execution.

| | **Local (No network cost)** | **Long Distance*** |
|---|---|---|
| Compute Cost | $0.28 | $0.35 |
| Total Cost ($/Signing) | $0.28 | $8.54 |

*Cost increases with distance because of increased network latency and data transfer costs (400 GiB of data), but allowed more parallelization of simultaneous scans.
Dual execution costs approximately twice as much.

## Related Works

Threshold cryptography based distributed certificate signing scheme has been proposed for bitcoins [1] which is resistant to collusion or node failures and takes around 13 s for a signing. More importantly, a two-party ECDSA signing scheme [2] has been proposed recently that takes 37 ms for signing using a 256 bit curve.

Though these schemes are efficient, they lack the flexibility of complex multi-party assertions during the certificate signing process. Our scheme achieves this flexibility using the MPC.

*[1] Rosario Gennaro, Steven Goldfeder and Arvind Narayanan, Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security, ACNS 2016*

*[2] Yehuda Lindell, Fast Secure Two-Party ECDSA Signing, 2017*