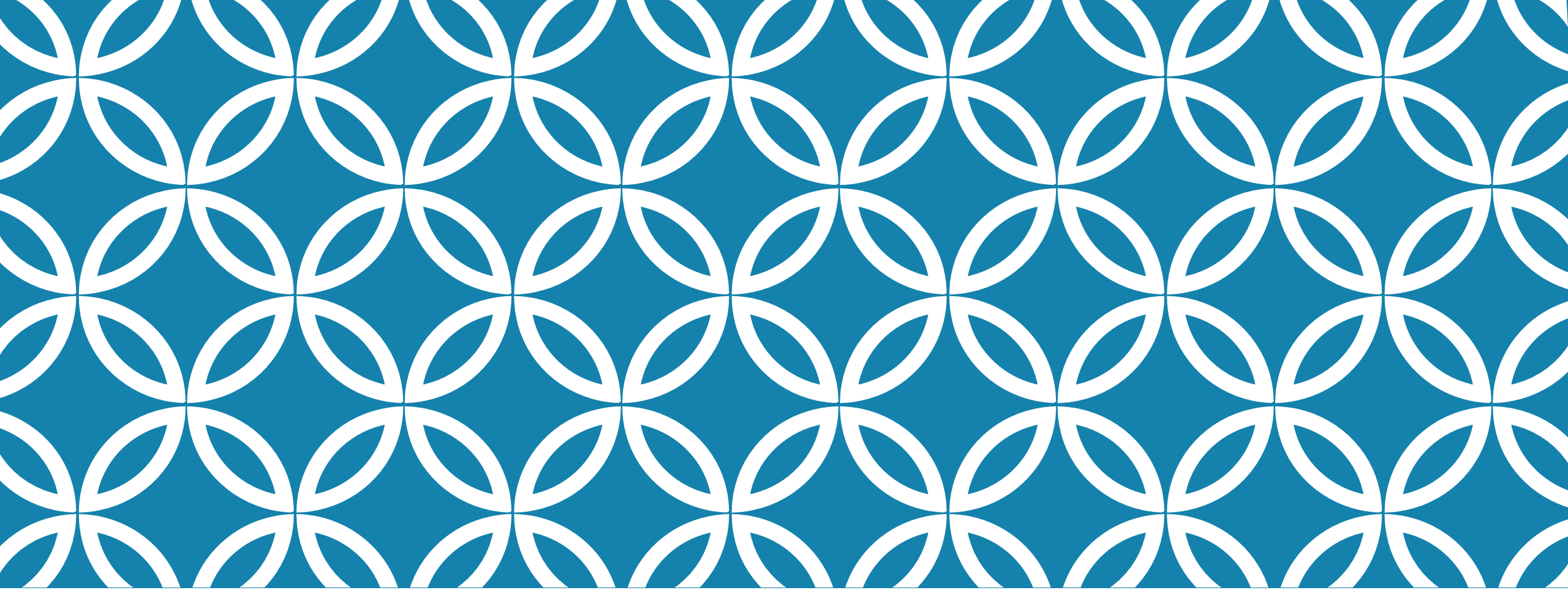


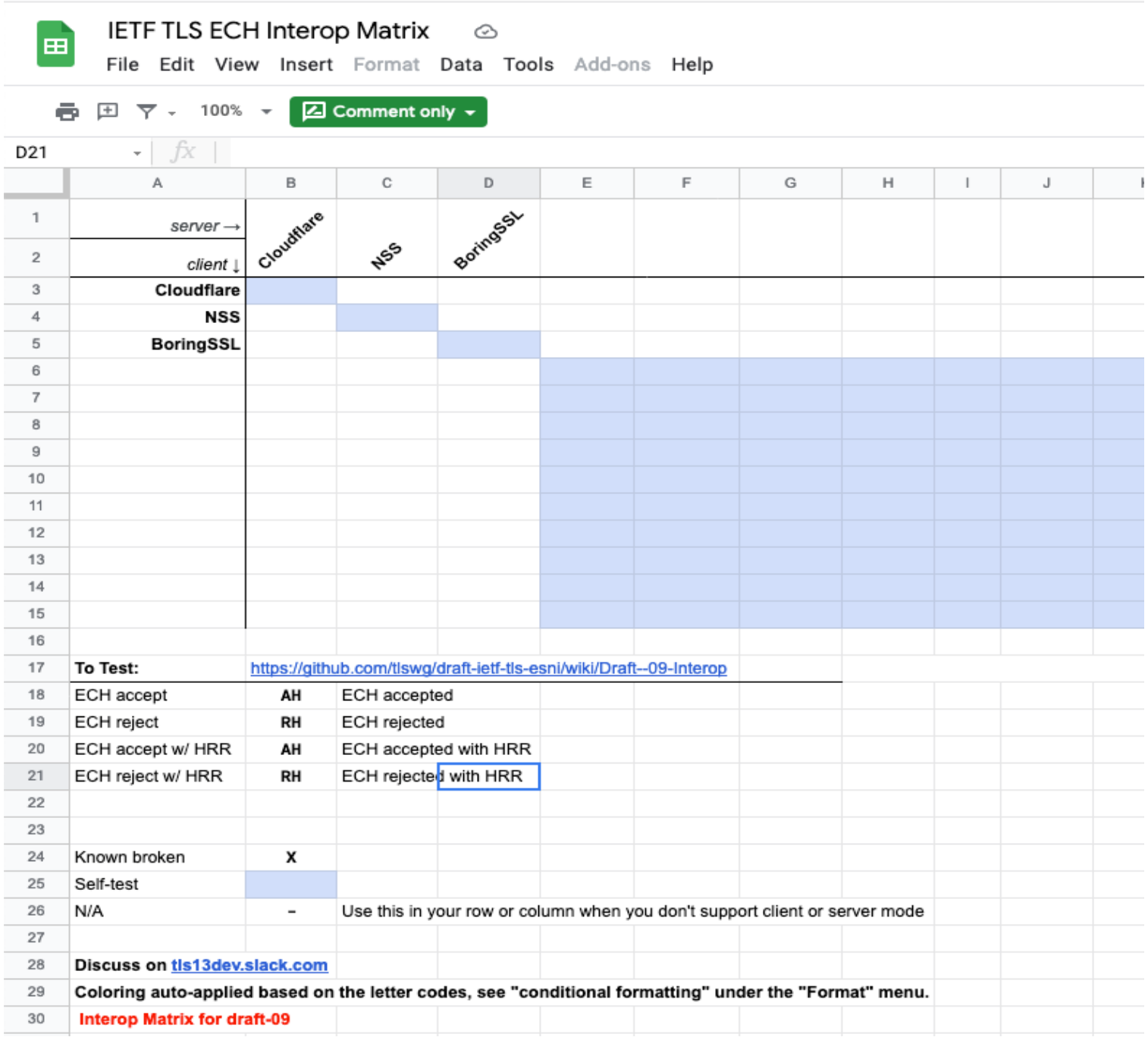
tls-interop-runner

Goutam Tamvada

UNIVERSITY OF WATERLOO

THE PROBLEM

Manually testing feature interoperability between TLS implementations is error-prone and does not scale



IETF TLS ECH Interop Matrix

File Edit View Insert Format Data Tools Add-ons Help

100% Comment only

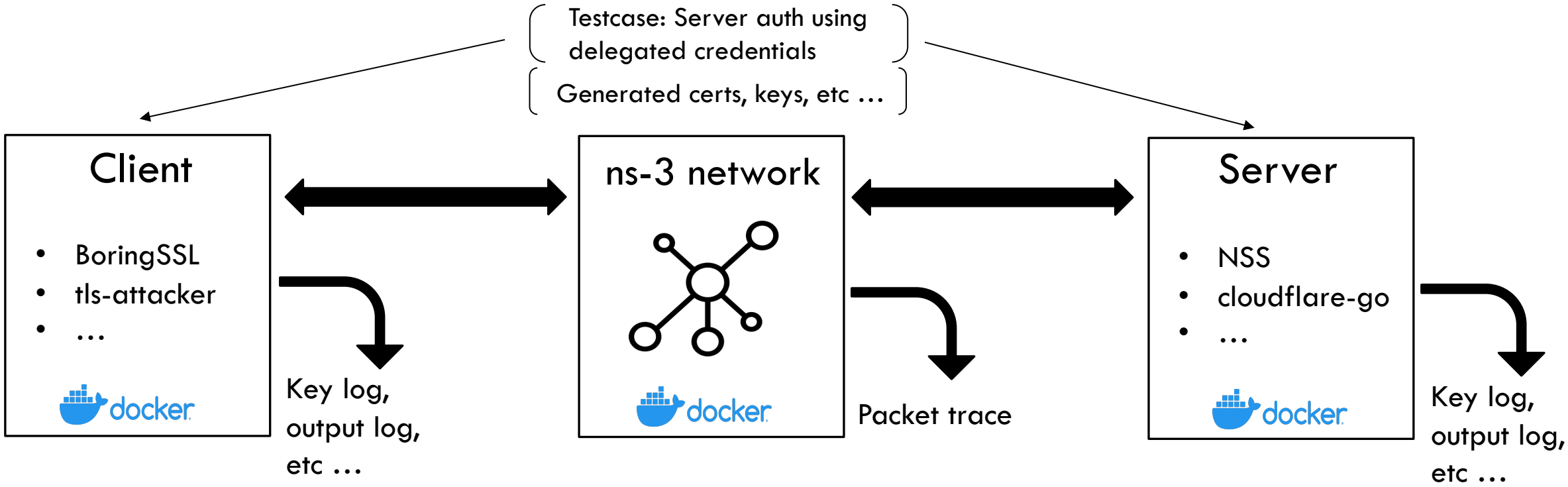
D21

	A	B	C	D	E	F	G	H	I	J
1	server →	Cloudflare	NSS	BoringSSL						
2	client ↓									
3	**Cloudflare**									
4	**NSS**									
5	**BoringSSL**									
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17	**To Test:**	https://github.com/tlswg/draft-ietf-tls-esni/wiki/Draft--09-Interop								
18	ECH accept	**AH**	ECH accepted							
19	ECH reject	**RH**	ECH rejected							
20	ECH accept w/ HRR	**AH**	ECH accepted with HRR							
21	ECH reject w/ HRR	**RH**	ECH rejected with HRR							
22										
23										
24	Known broken	**X**								
25	Self-test									
26	N/A	-	Use this in your row or column when you don't support client or server mode							
27										
28	**Discuss on tls13dev.slack.com**									
29	**Coloring auto-applied based on the letter codes, see "conditional formatting" under the "Format" menu.**									
30	**Interop Matrix for draft-09**									

https://docs.google.com/spreadsheets/d/1vti74lIN25stdyv8cuW7zHUHI3J7_DkkSdj3ECT2kIM/edit#gid=607315625

SOLUTION: tls-interop-runner

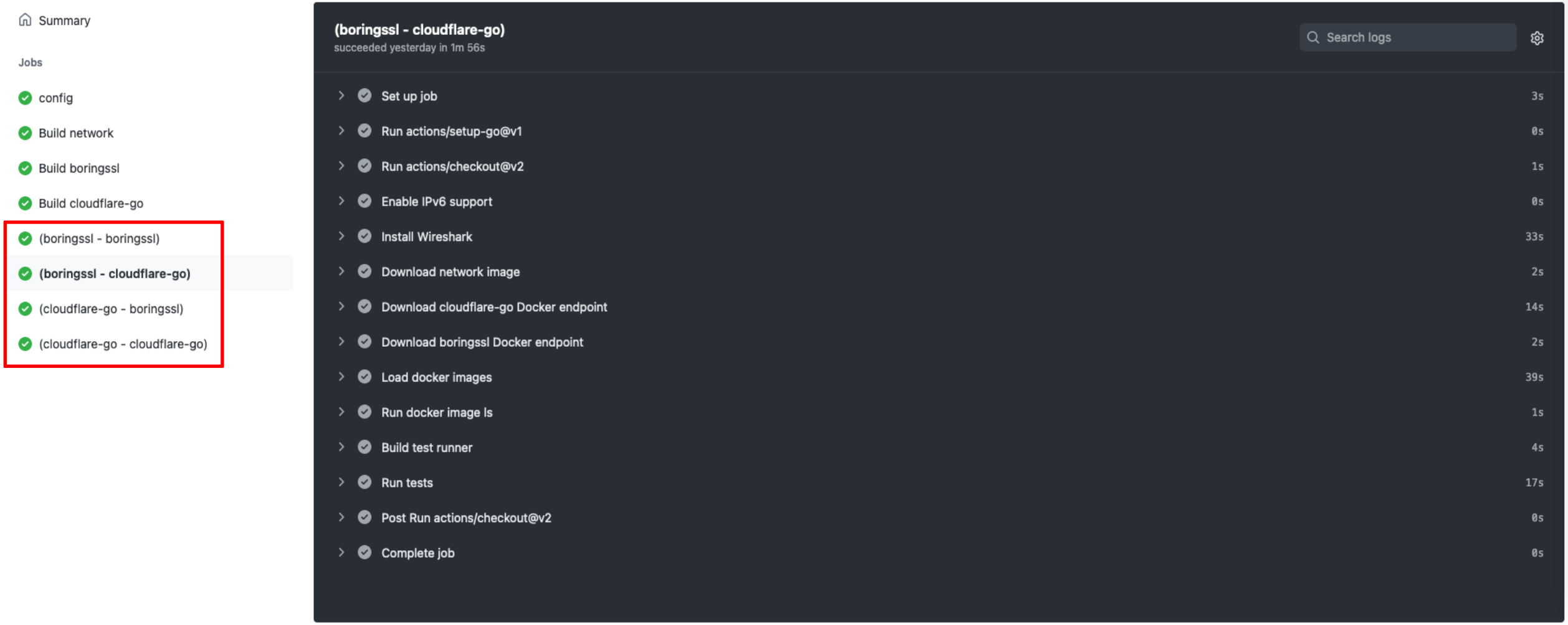
(Inspired by https://github.com/marten-seemann/quic-interop-runner)



Adding new endpoints and testcases is easy!

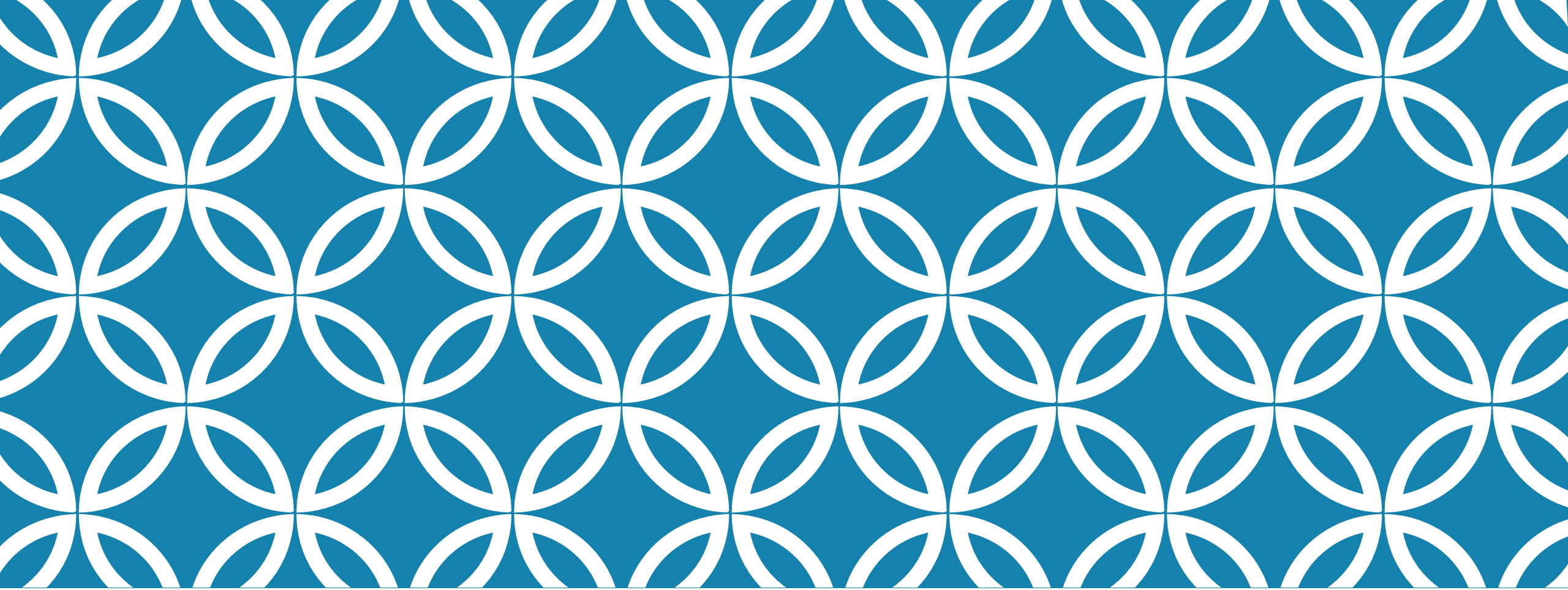
Docker logo from https://www.docker.com/company/newsroom/media-resources, network icon from https://www.flaticon.com/free-icon/network_149181

DEMO


Summary
Jobs
config
Build network
Build boringssl
Build cloudflare-go
(boringssl - boringssl)
(boringssl - cloudflare-go)
(cloudflare-go - boringssl)
(cloudflare-go - cloudflare-go)
(boringssl - cloudflare-go)
succeeded yesterday in 1m 56s
Search logs
Set up job 3s
Run actions/setup-go@v1 0s
Run actions/checkout@v2 1s
Enable IPv6 support 0s
Install Wireshark 33s
Download network image 2s
Download cloudflare-go Docker endpoint 14s
Download boringssl Docker endpoint 2s
Load docker images 39s
Run docker image ls 1s
Build test runner 4s
Run tests 17s
Post Run actions/checkout@v2 0s
Complete job 0s

IN SUM

- tls-interop-runner is an **automated TLS interoperability testing framework**, inspired by the QUIC Interop Runner
- To eventually include fuzz, performance, and regression testing
- Can be cloned from **https://github.com/xvzcf/tls-interop-runner** and run locally **(Website coming soon!)**
- MIT License**: Pull requests and issues welcome!**



tls-interop-runner

Goutam Tamvada

UNIVERSITY OF WATERLOO