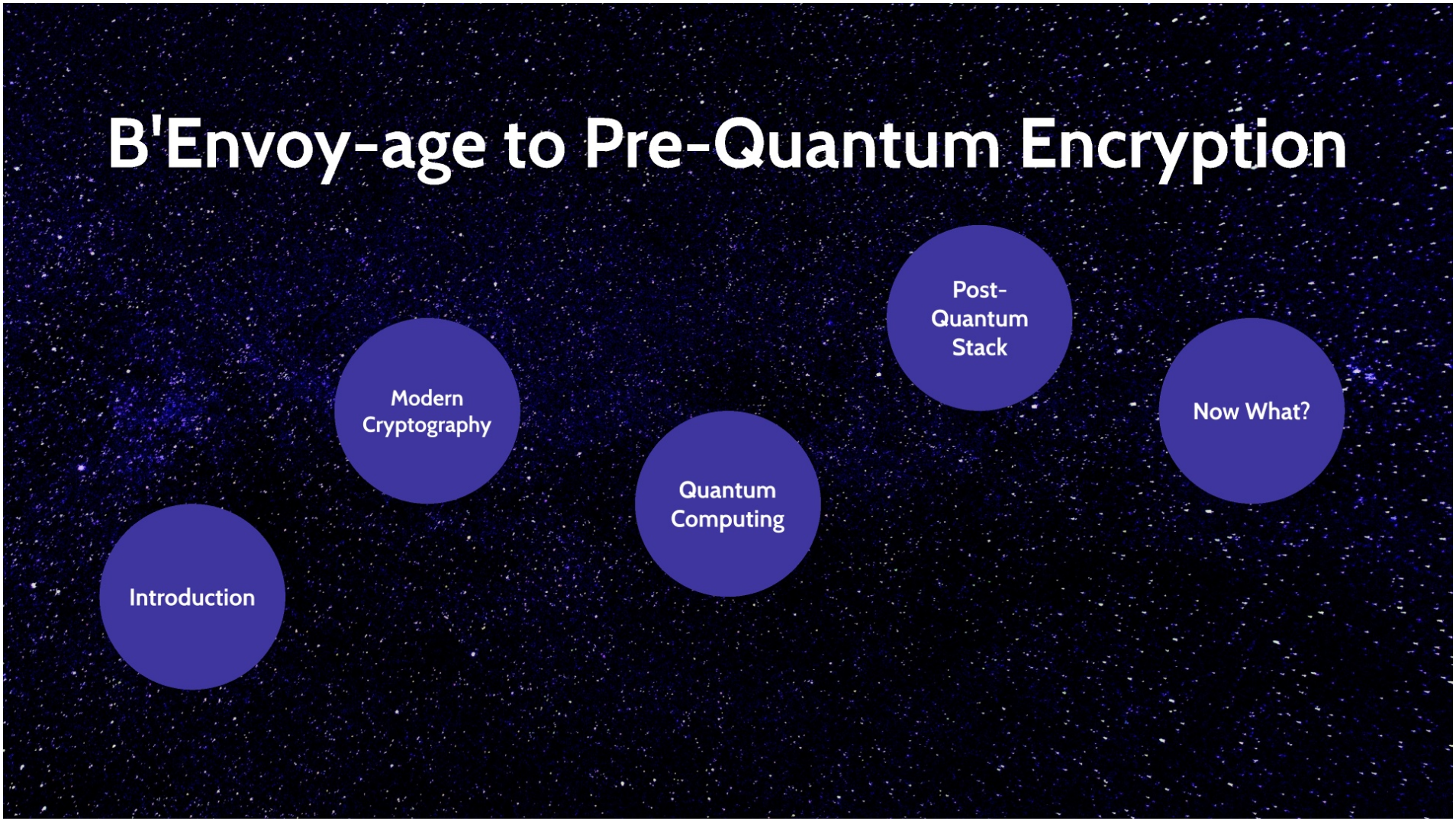

B'Envoy-age to Pre-Quantum Encryption
Introduction
Modern Cryptography
Quantum Computing
Post-Quantum Stack
Now What?

Team

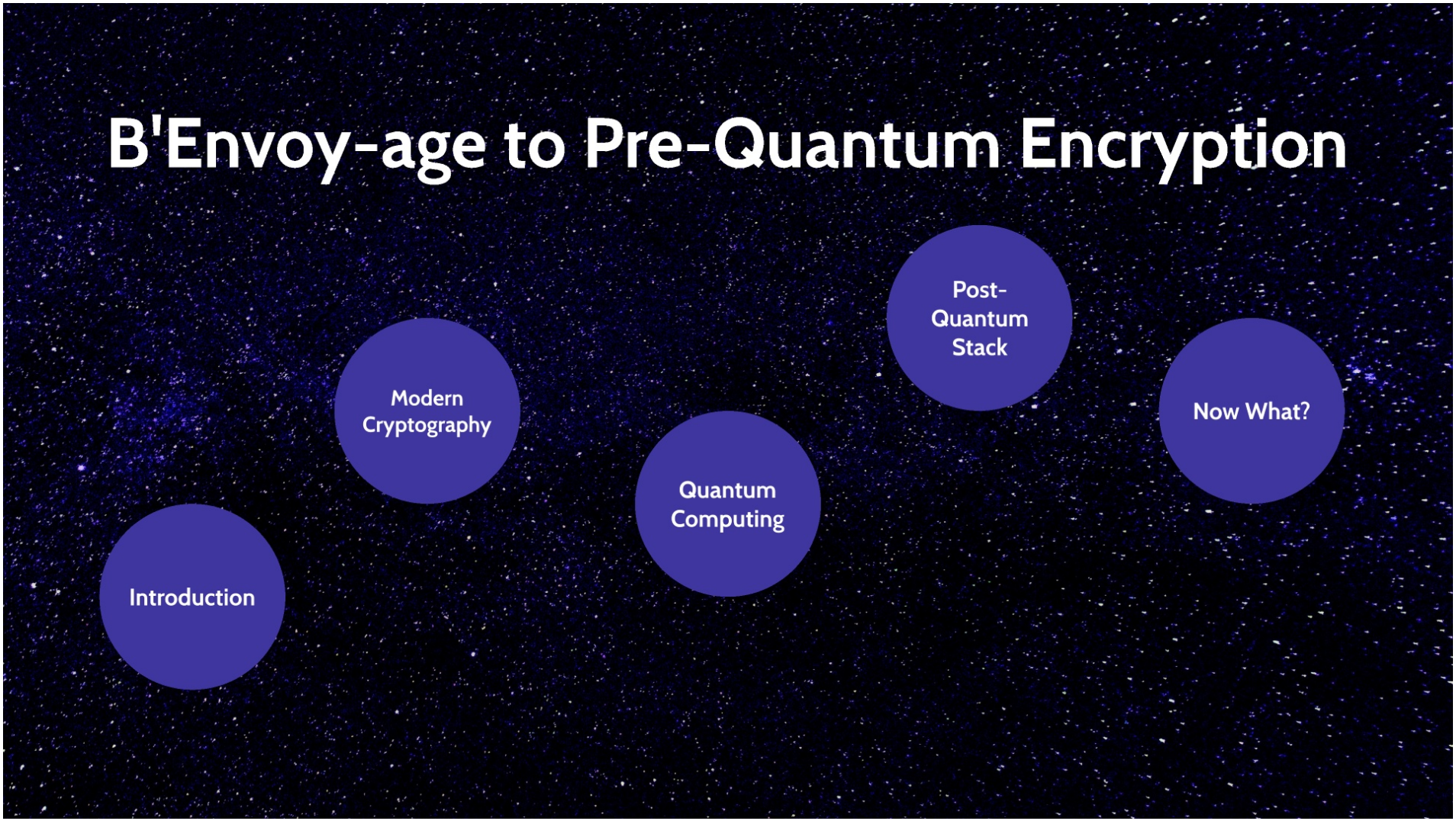
Emma Dickenson

Daniel Rouhana

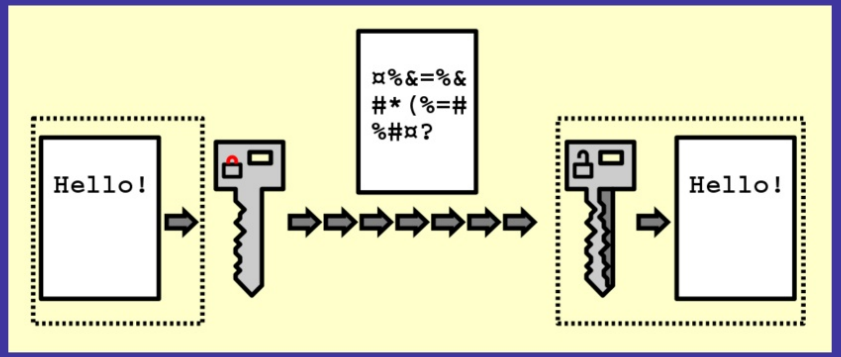
Doron Podoleanu

Why attend this talk?

- What is quantum computing?
- What does "post-quantum" mean?
- Post quantum cloud native stack: PQ Istio, demos, future plans


B'Envoy-age to Pre-Quantum Encryption
Introduction
Modern Cryptography
Quantum Computing
Post-Quantum Stack
Now What?

Modern Cryptography

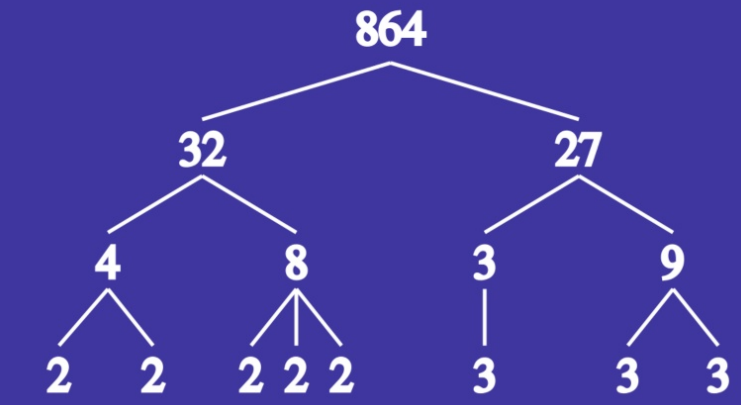


(Wikipedia)

Why is Encryption "Secure?"

- Computational intractability
- RSA
  - 2048 bit key

$$n = p \cdot q$$

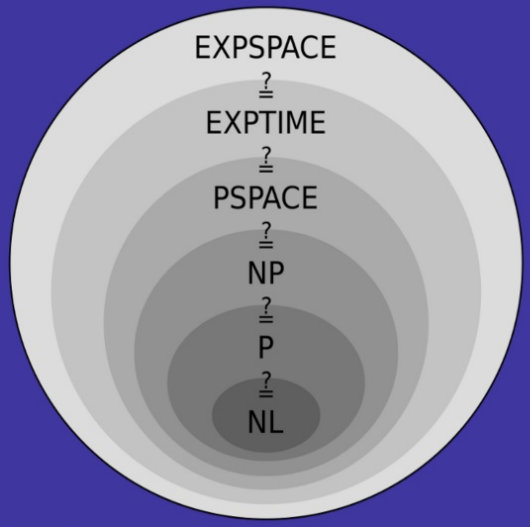


(Wikipedia)

Not All Problems Are Created Equal

"Hard" problems to solve:

- Integer factorization problem (NP)
- Discrete logarithm problem (NP, "coNP")
- Elliptic-curve discrete logarithm problem

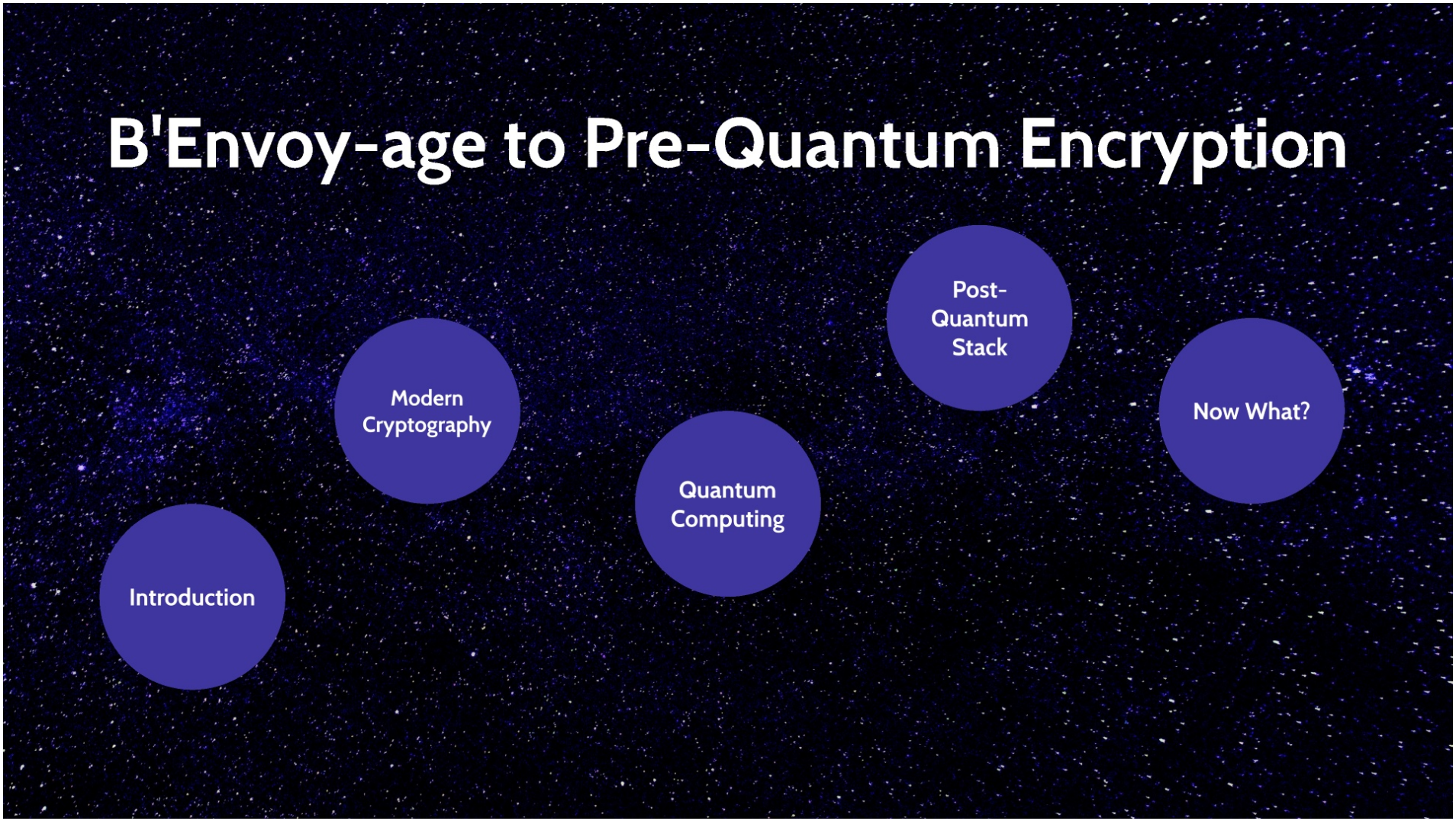


(Wikipedia)

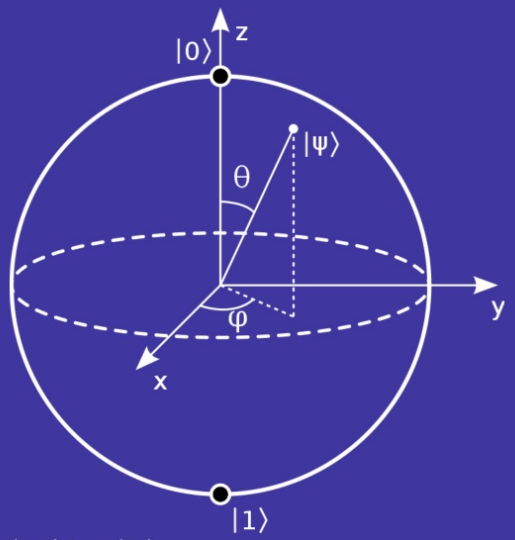
Current Industry Standard

Key exchange/agreement and authentication							
Algorithm	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	Status
RSA	Yes	Yes	Yes	Yes	Yes	No	
DH-RSA	No	Yes	Yes	Yes	Yes	No	
DHE-RSA (forward secrecy)	No	Yes	Yes	Yes	Yes	Yes	
ECDH-RSA	No	No	Yes	Yes	Yes	No	
ECDHE-RSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes	
DH-DSS	No	Yes	Yes	Yes	Yes	No	
DHE-DSS (forward secrecy)	No	Yes	Yes	Yes	Yes	No[58]	
ECDH-ECDSA	No	No	Yes	Yes	Yes	No	
ECDHE-ECDSA (forward secrecy)	No	No	Yes	Yes	Yes	Yes	
ECDH-EdDSA	No	No	Yes	Yes	Yes	No	
ECDHE-EdDSA (forward secrecy)[59]	No	No	Yes	Yes	Yes	Yes	Defined for TLS 1.2 in RFCs
PSK	No	No	Yes	Yes	Yes	?	
PSK-RSA	No	No	Yes	Yes	Yes	?	
DHE-PSK (forward secrecy)	No	No	Yes	Yes	Yes	Yes	
ECDHE-PSK (forward secrecy)	No	No	Yes	Yes	Yes	Yes	
SRP	No	No	Yes	Yes	Yes	?	
SRP-DSS	No	No	Yes	Yes	Yes	?	
SRP-RSA	No	No	Yes	Yes	Yes	?	
Kerberos	No	No	Yes	Yes	Yes	?	
DH-ANON (insecure)	No	Yes	Yes	Yes	Yes	?	
ECDH-ANON (insecure)	No	No	Yes	Yes	Yes	?	
GOST R 34.10-94/34.10-2001[60]	No	No	Yes	Yes	Yes	?	Proposed in RFC drafts

(Wikipedia)

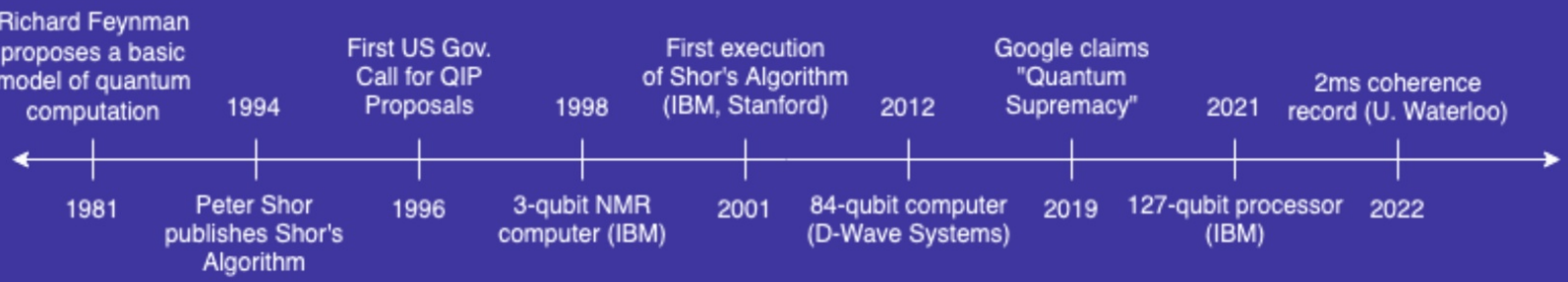

B'Envoy-age to Pre-Quantum Encryption
Introduction
Modern Cryptography
Quantum Computing
Post-Quantum Stack
Now What?

Quantum Computing: A Brief, Unsatisfying, and Uncomprehensive Overview

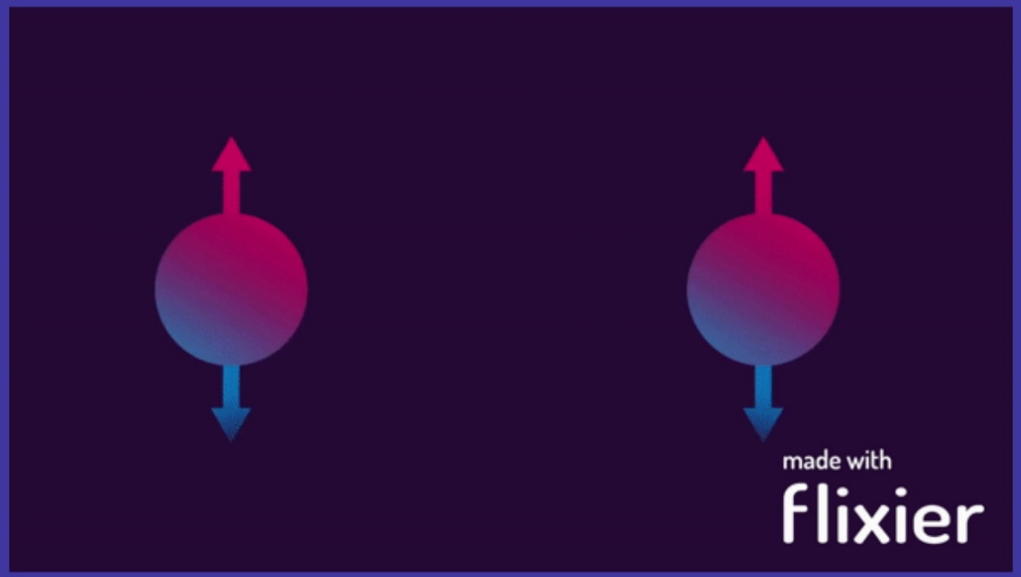


(Wikipedia)

History

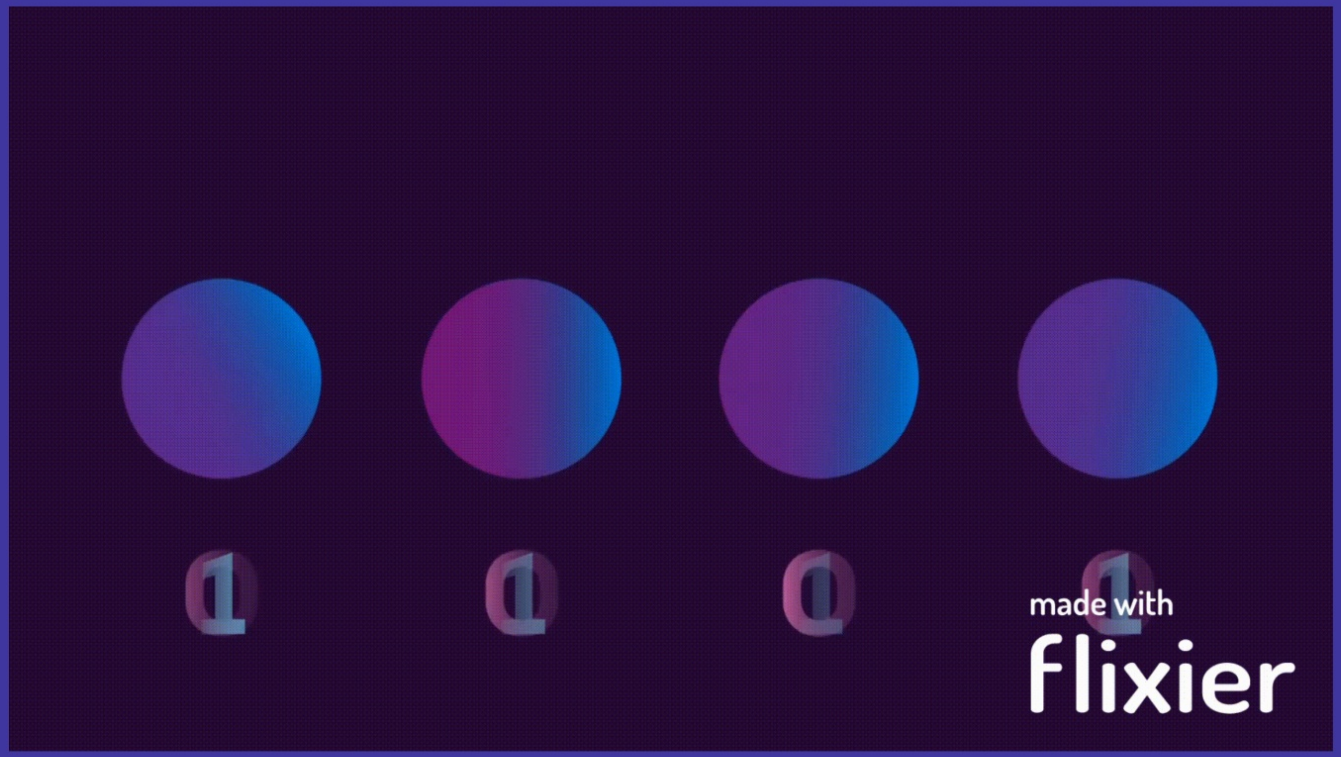

Richard Feynman proposes a basic model of quantum computation
1981
1994
Peter Shor publishes Shor's Algorithm
First US Gov. Call for QIP Proposals
1996
1998
3-qubit NMR computer (IBM)
First execution of Shor's Algorithm (IBM, Stanford)
2001
2012
84-qubit computer (D-Wave Systems)
Google claims "Quantum Supremacy"
2019
2021
127-qubit processor (IBM)
2ms coherence record (U. Waterloo)
2022

Entanglement



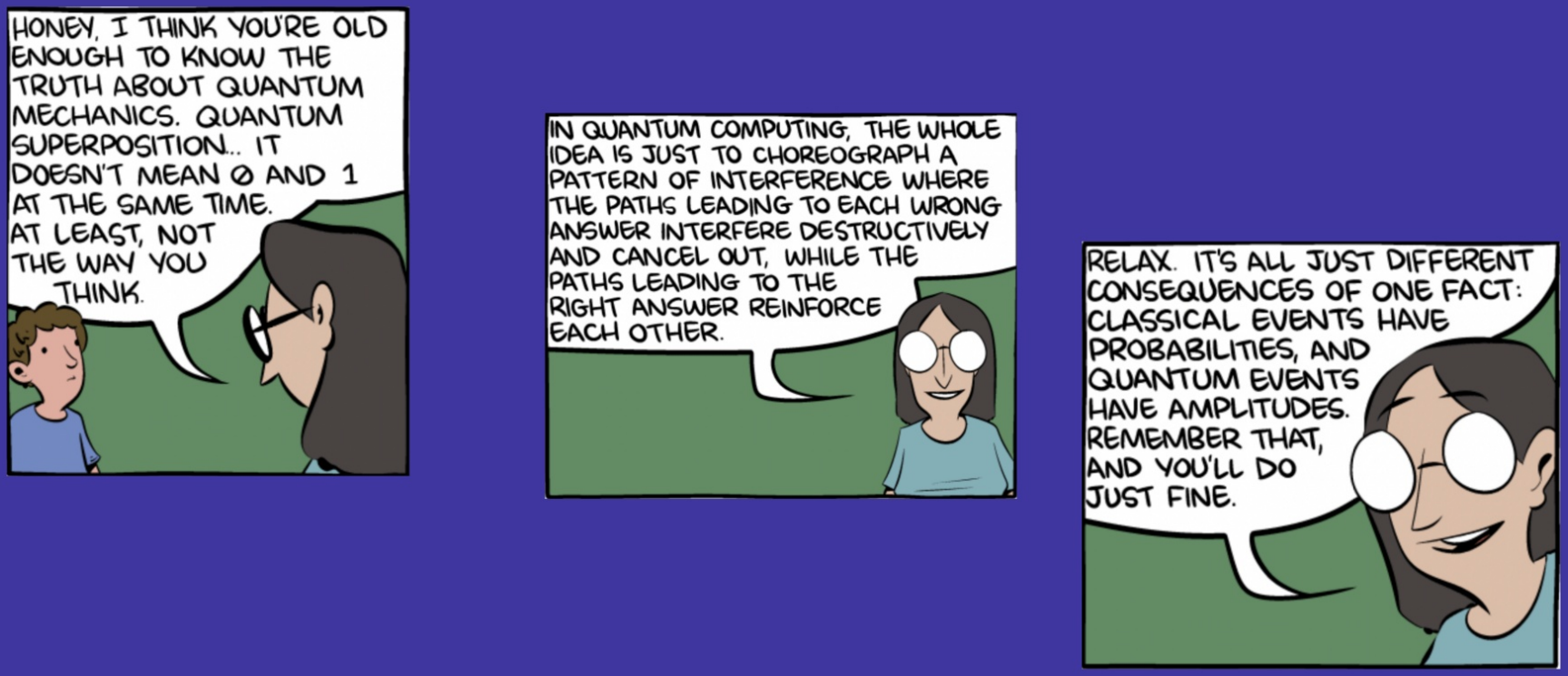
"Spooky action at a distance"
- Albert Einstein

Superposition



Superposition

Quantum Computation



("The Talk," Scott Aaronson and Zach Weinersmith)

Superposition: Qbits

Classical Bits:

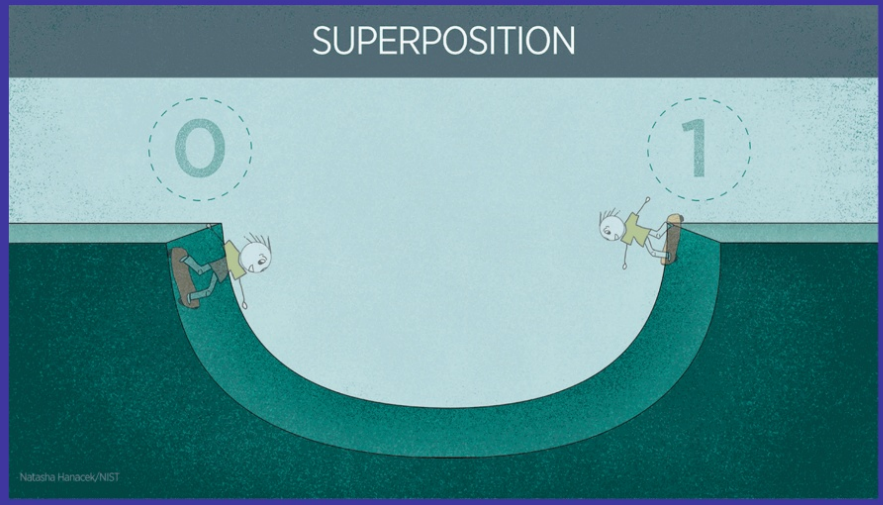
$$\begin{pmatrix}1\\0\end{pmatrix} \qquad \begin{pmatrix}0\\1\end{pmatrix}$$

$$0 \qquad 1$$

Quantum Bits (Qbits):

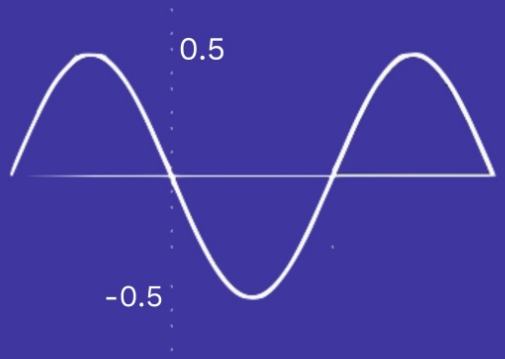
$$\begin{pmatrix}a\\b\end{pmatrix} \qquad a, b \in \mathbb{C}$$

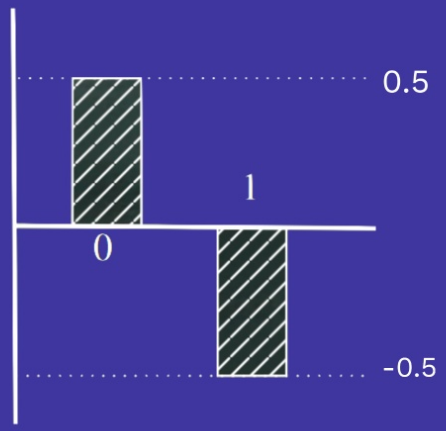
$$||a||^2 + ||b||^2 = 1$$

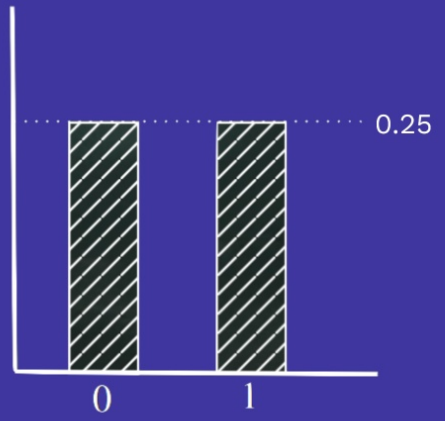


(Becoming Human: Artificial Intelligence Magazine)

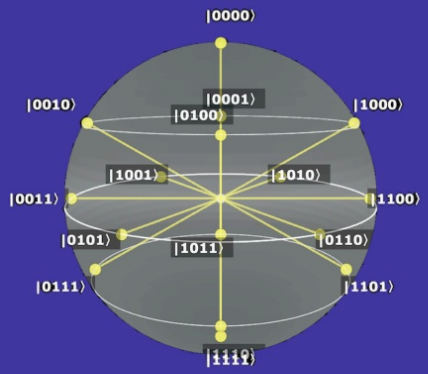
Probability Intuition



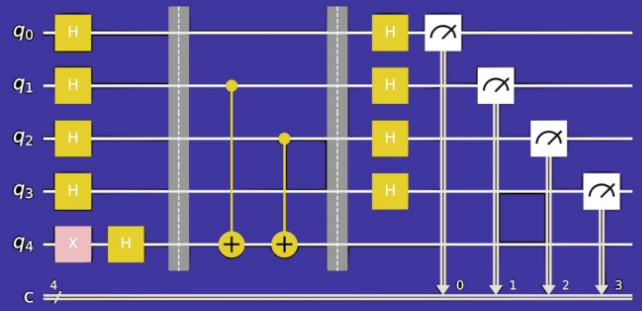




Probability Amplitudes

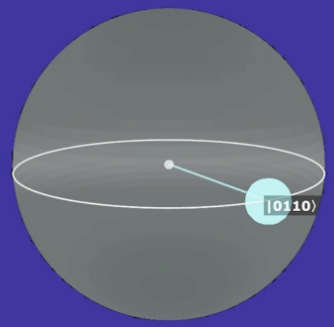


Superposition of all possibilities



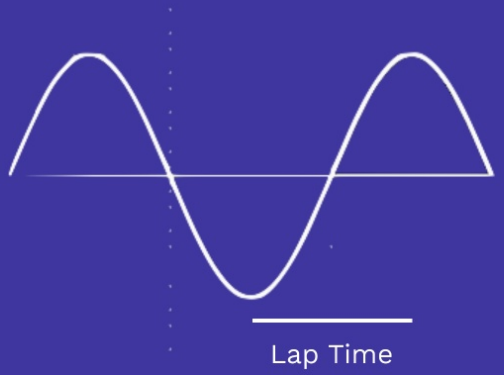
Computation driven interference

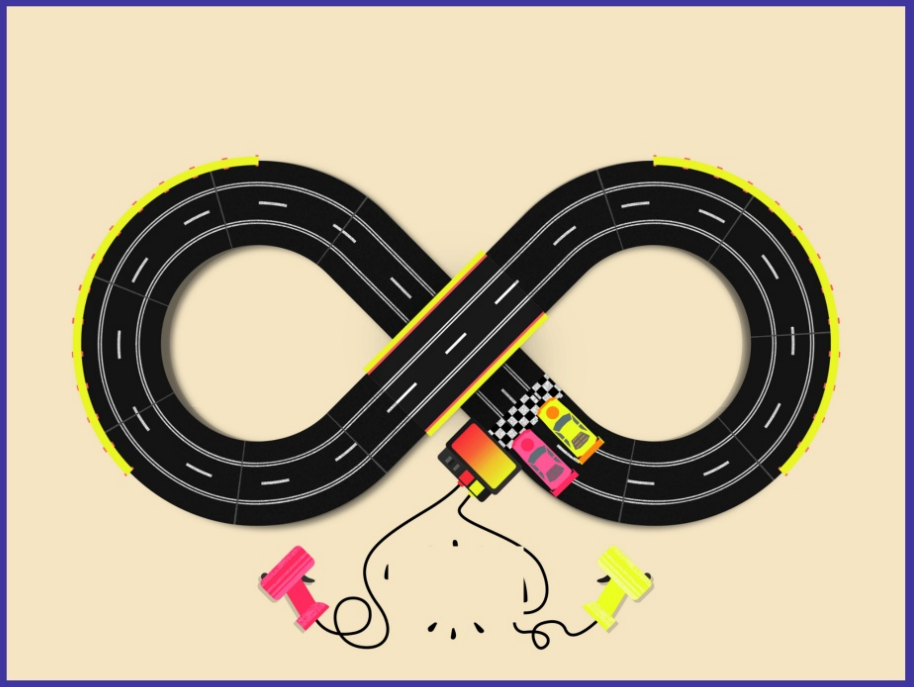
(Qiskit)



Solution

Cracking Encryption





Quantum Computing Currently

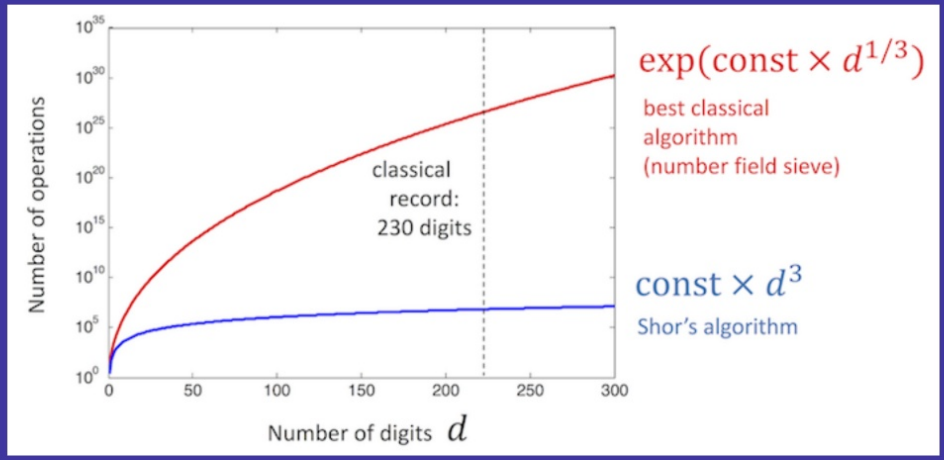
- Leaky qbits
- "Fault-tolerant" quantum computing
- National security initiatives

quantum.gov

The Quantum Problem

Shor's Algorithm: from factoring to period finding

- Integer factorization
- Discrete logarithm
- Elliptic-curve discrete logarithm



(IBM Quantum)

Quantifying Speed-up

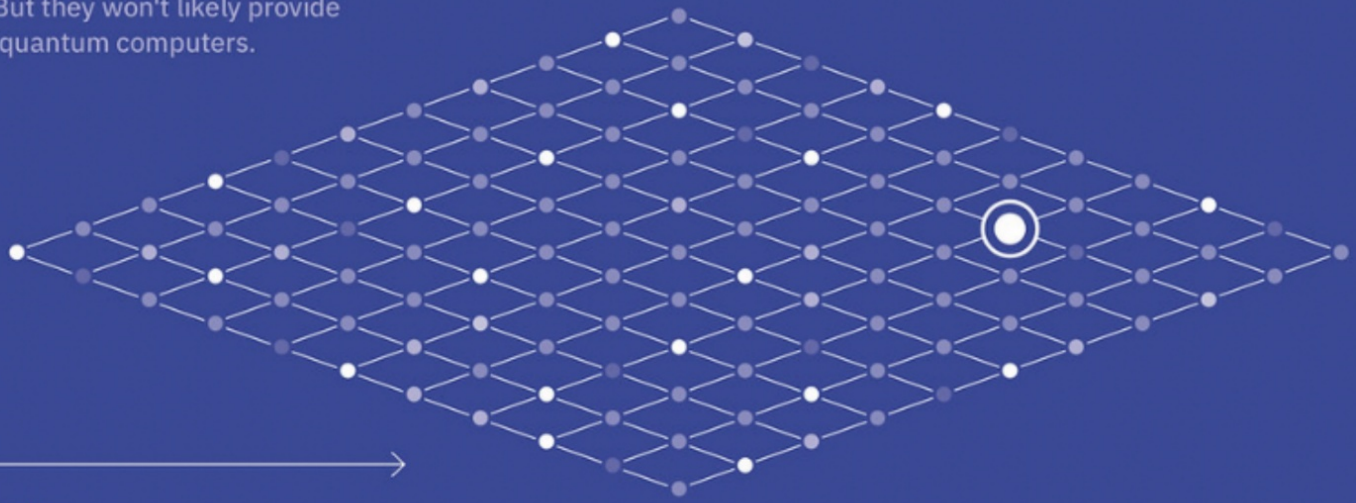
n	n_e	Parameters d_1	d_2	δ_{off}	c_{mul}	c_{exp}	c_{sep}	Retry Risk	Volume (megaqubitdays) per run	expected	Qubits (megaqubits) per run	Runtime (hours) per run
1024	$3(n/2-1)-40$	15	27	5	5	5	1024	6%	0.5	0.5	9.7	1.3
2048		15	27	4	5	5	1024	31%	4.1	5.9	20	5.1
3072		17	29	6	4	5	1024	9%	19	21	38	12
4096		17	31	9	4	5	1024	5%	48	51	55	22
8192		19	33	4	4	5	1024	5%	480	510	140	86
12288		19	33	3	4	5	1024	12%	1700	1900	200	200
16384		19	33	4	4	5	1024	24%	3900	5100	270	350

"How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits" Gidney, Ekera (2017)


Cryptography
Today and Tomorrow
Today's status quo crytpography paradigm, which relies on prime factorization, may be sufficiently difficult to crack today. But they won't likely provide safety against powerful quantum computers.
TODAY'S CRYPTOGRAPHY
Today's cryptosystems, including RSA and Diffie-Hellman, rely on prime factorization, a scheme in which mathematical constructs conceal and secure keys.
CRYPTOGRAPHY FOR THE QUANTUM AGE
Lattice-based cryptography moves beyond prime factoring of large numbers and hides a the key in a high-dimensional lattice. Solving the mathematical problems required to unveil a key in such a lattice is considered likely impossible, even by futuristic quantum machines.
SOURCE _ IBM RESEARCH

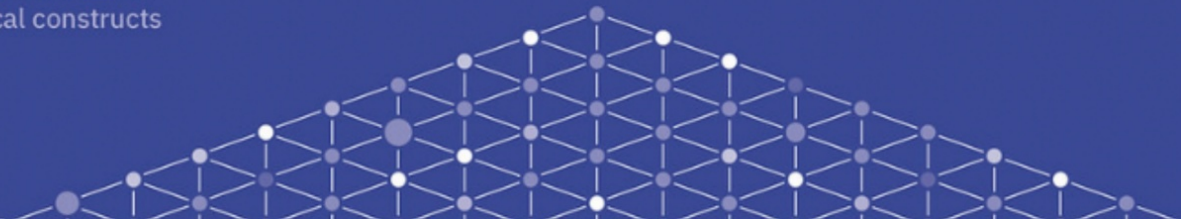
Cryptography
Today and Tomorrow

Today's status quo crytpography paradigm, which relies on prime factorization, may be sufficiently difficult to crack today. But they won't likely provide safety against powerful quantum computers.

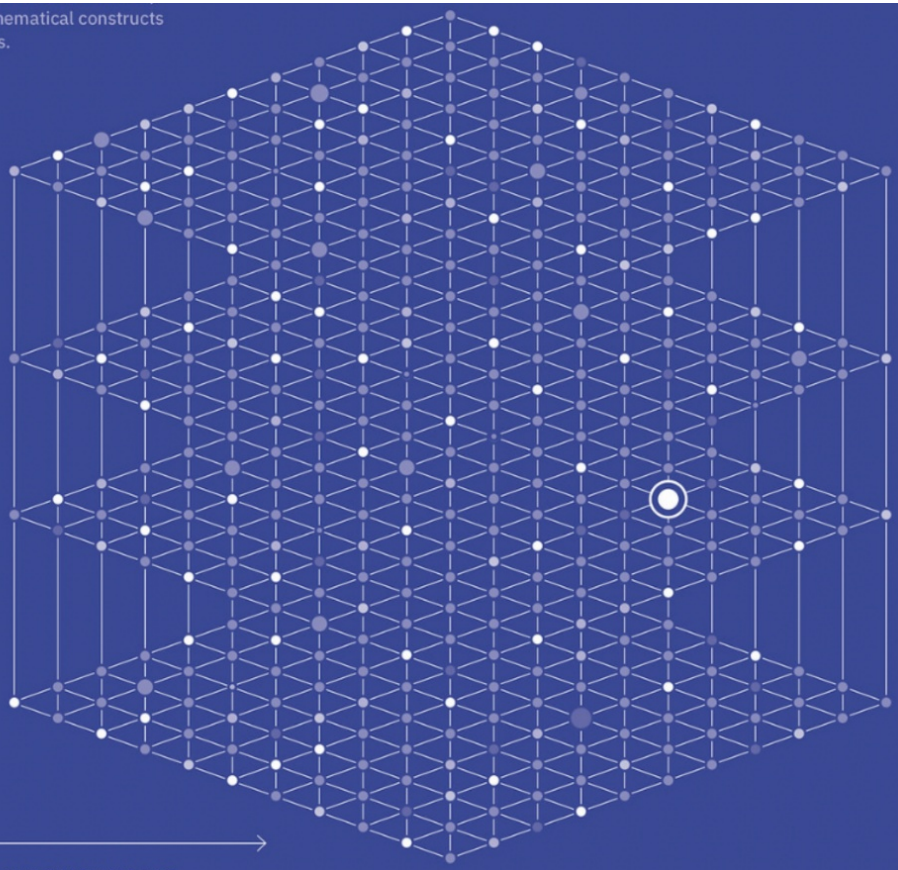


TODAY'S CRYPTOGRAPHY

Today's cryptosystems, including RSA and Diffie-Hellman. rely on prime factorization, a scheme in which mathematical constructs conceal and secure keys.



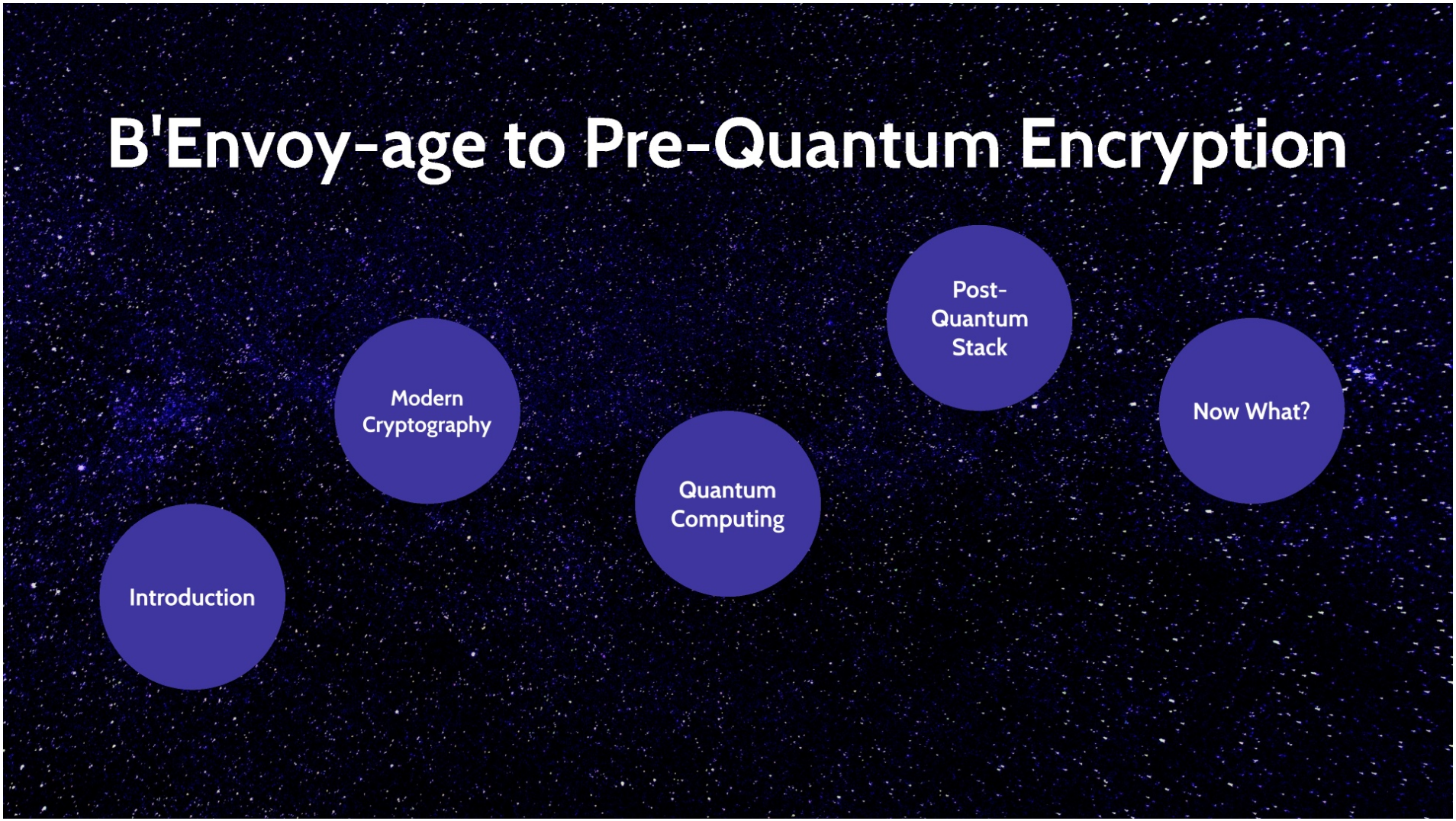
a scheme in which mathematical constructs conceal and secure keys.



CRYPTOGRAPHY FOR THE QUANTUM AGE

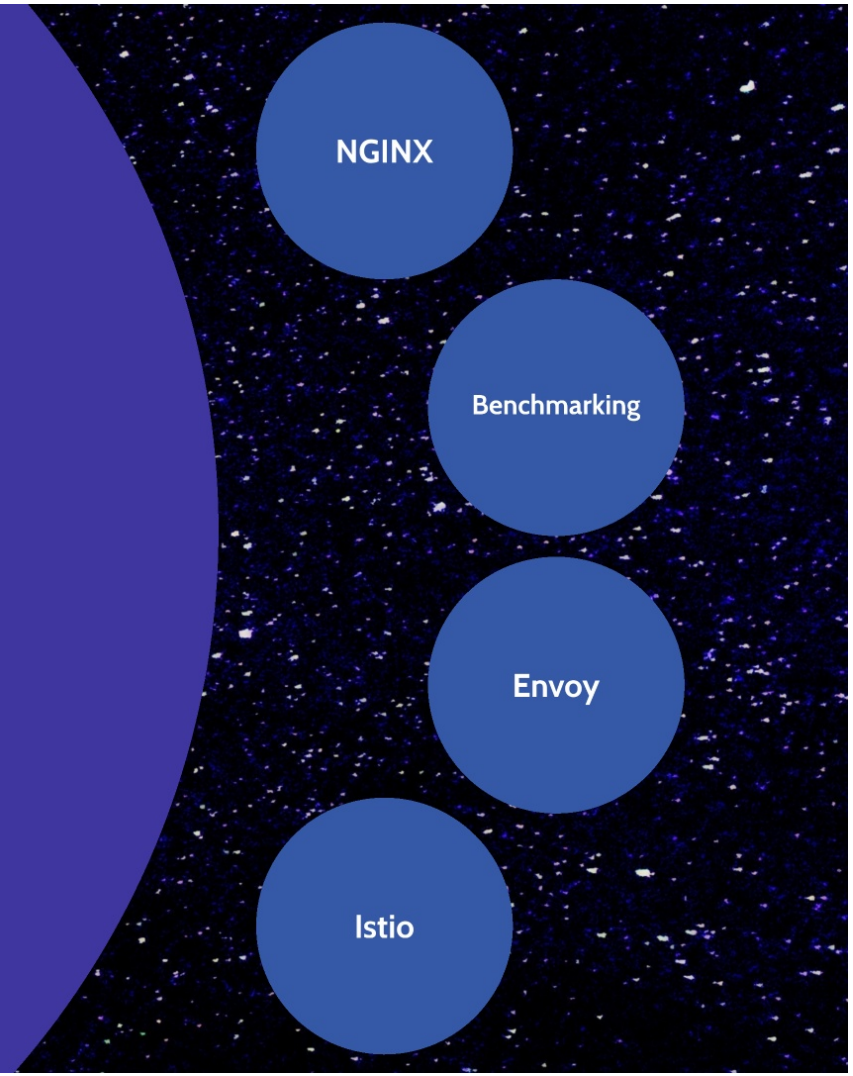
Lattice-based cryptography moves beyond prime factoring of large numbers and hides a the key in a high-dimensional lattice. Solving the mathematical problems required to unveil a key in such a lattice is considered likely impossible, even by futuristic quantum machines.

SOURCE _ IBM RESEARCH


B'Envoy-age to Pre-Quantum Encryption
Introduction
Modern Cryptography
Quantum Computing
Post-Quantum Stack
Now What?

Post-Quantum Stack

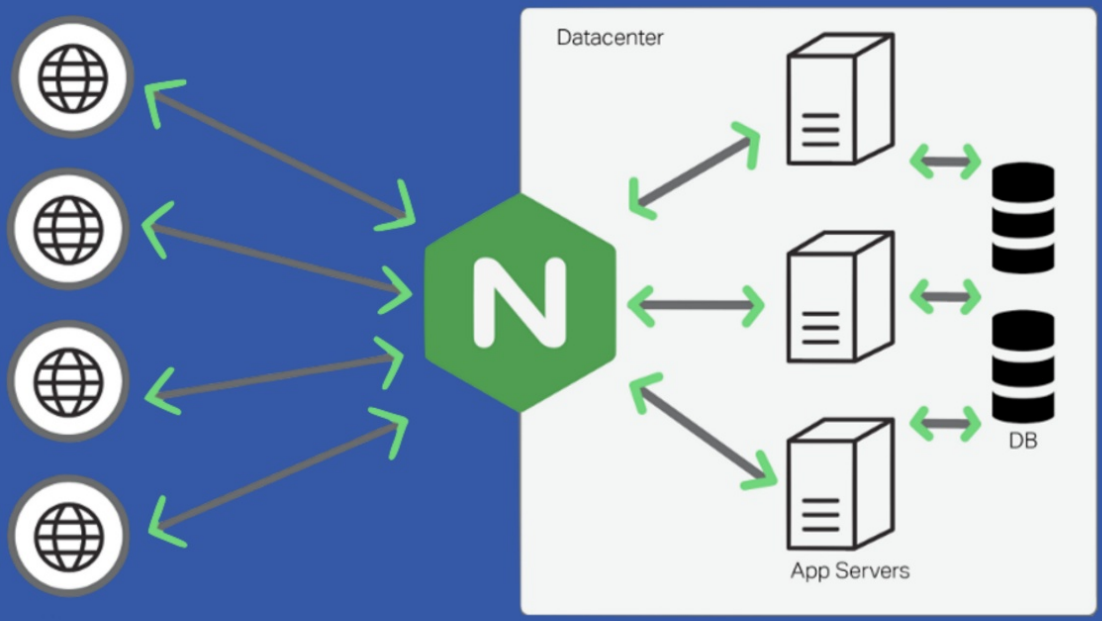
- OpenQuantumSafe library
- NGINX v1.20
- Envoy v1.23.1
- Istio v1.25
- Kubernetes v1.25
- Minikube v1.27
- BoringSSL-OQS



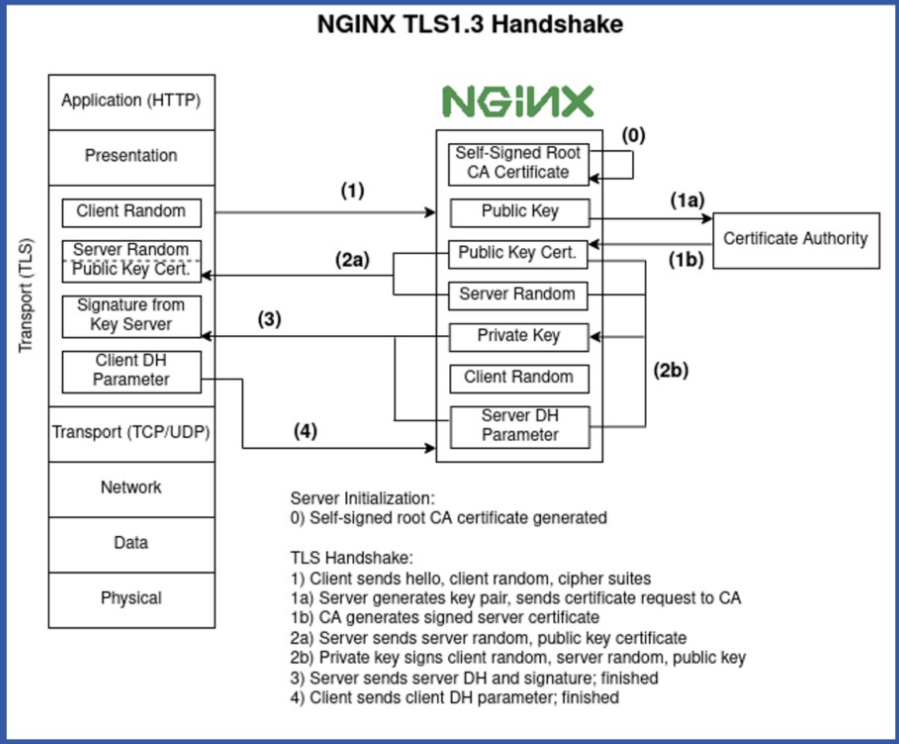
NGINX

Functionalities:

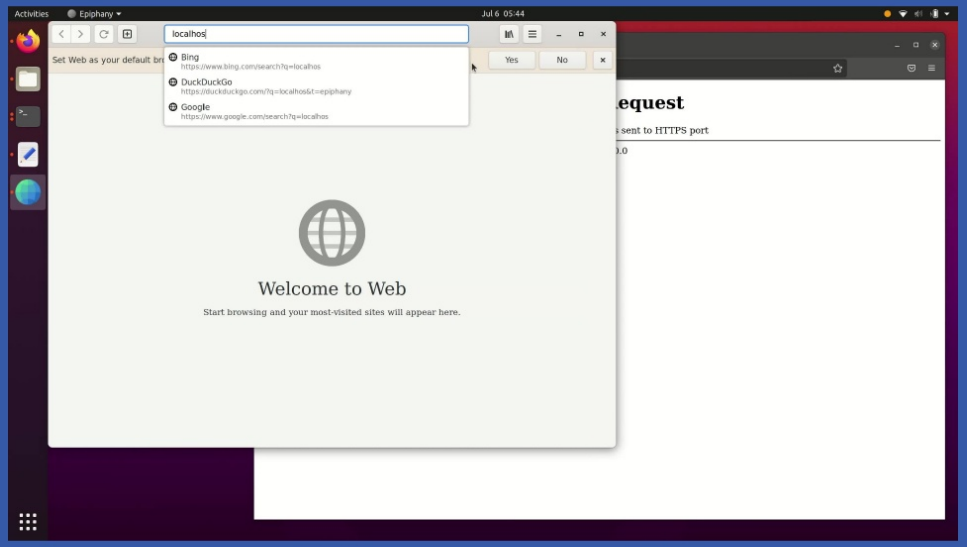
- Reverse proxy
- Load balancer
- HTTP cache
- Media streaming

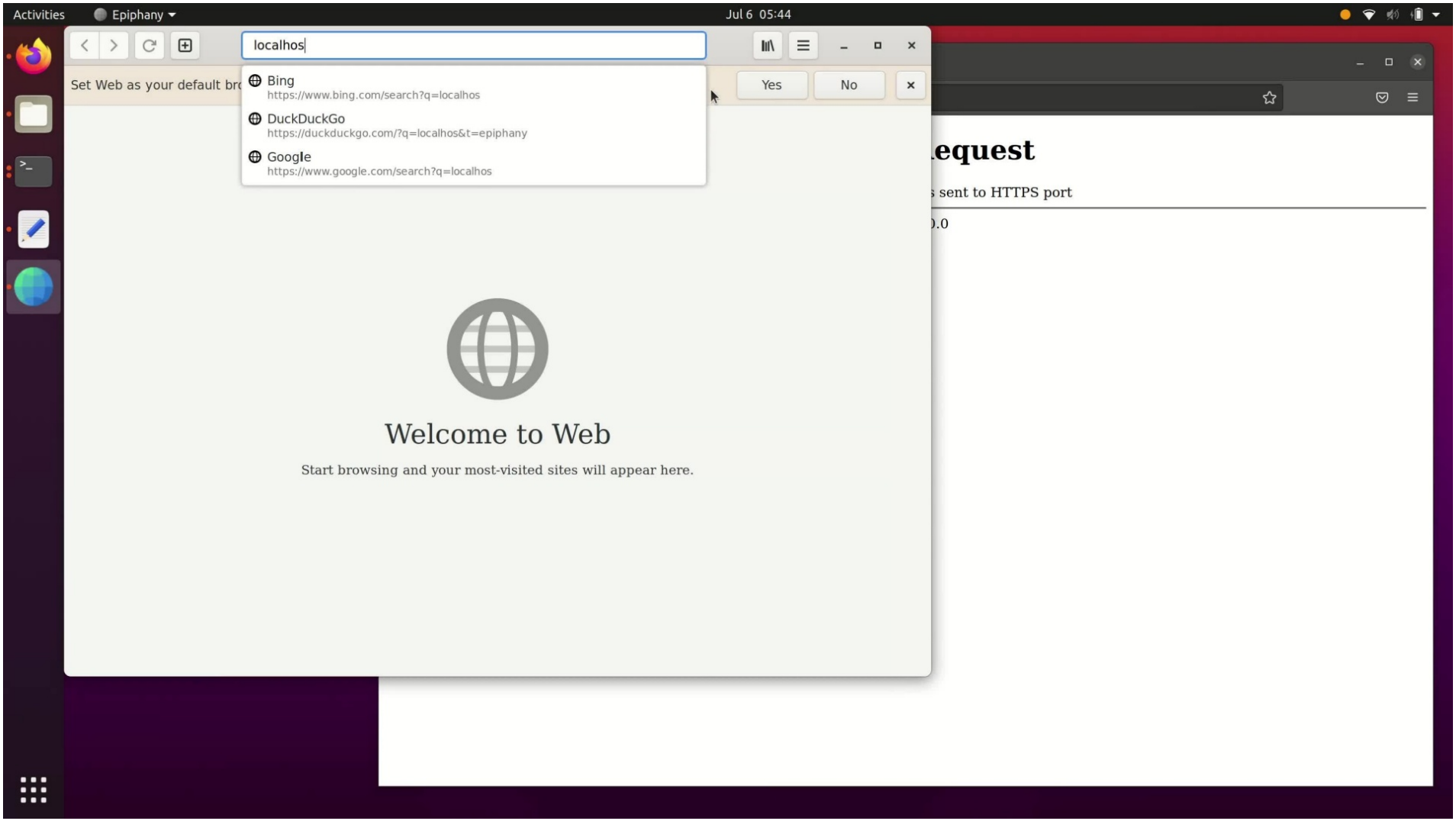


Transport Layer Security (TLS)



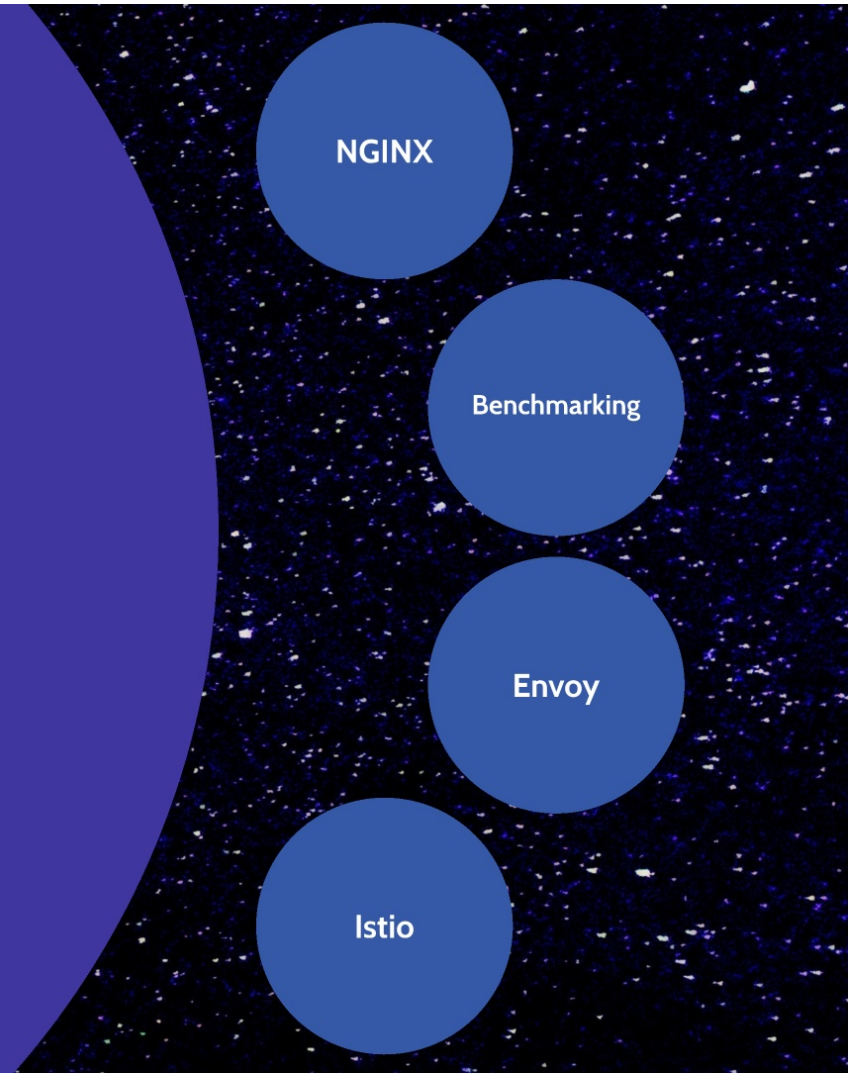
NGINX TLS Demo




Activities
Epiphany
Jul 6 05:44
localhos
Bing
https://www.bing.com/search?q=localhos
DuckDuckGo
https://duckduckgo.com/?q=localhos&t=epiphany
Google
https://www.google.com/search?q=localhos
Set Web as your default br
Yes
No
Welcome to Web
Start browsing and your most-visited sites will appear here.
equest
sent to HTTPS port
.0

Post-Quantum Stack

- OpenQuantumSafe library
- NGINX v1.20
- Envoy v1.23.1
- Istio v1.25
- Kubernetes v1.25
- Minikube v1.27
- BoringSSL-OQS



Benchmarking

NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

Federal agency reveals the first group of winners from its six-year competition.

July 05, 2022

The first four algorithms NIST has announced for post-quantum cryptography are based on structured lattices and hash functions, two families of math problems that could resist a quantum computer's assault.
Credit: N. Hanacek/NIST

GAITHERSBURG, Md. — The U.S. Department of Commerce's National Institute of Standards and Technology (NIST)

MEDIA CONTACT

Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS

Information Technology Laboratory
Computer Security Division
Cryptographic Technology Group

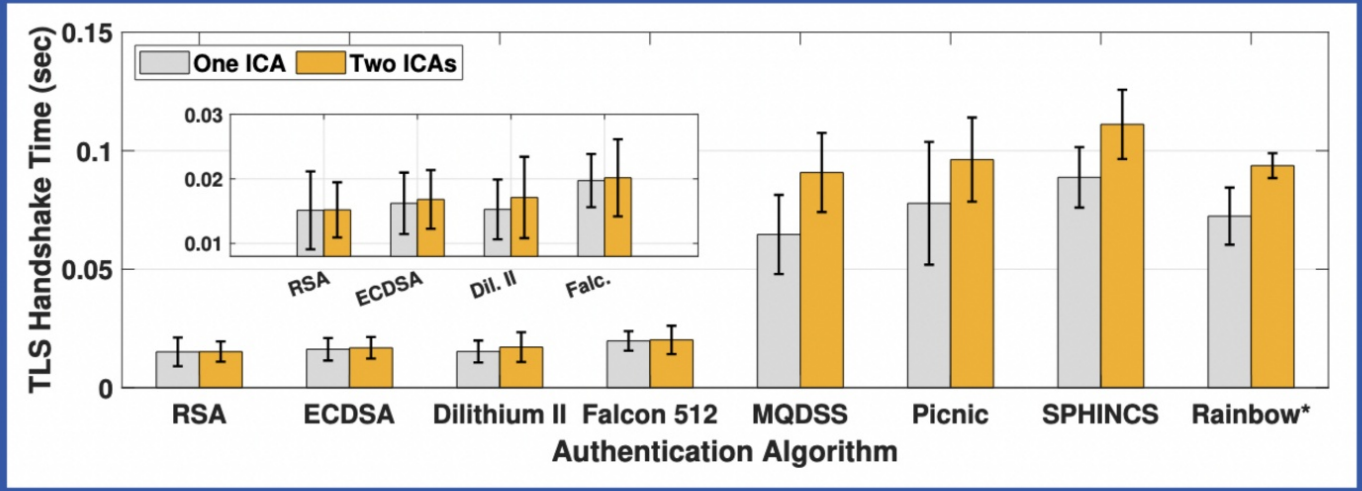
RELATED PUBLICATIONS

Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

SIGN UP FOR UPDATES FROM NIST

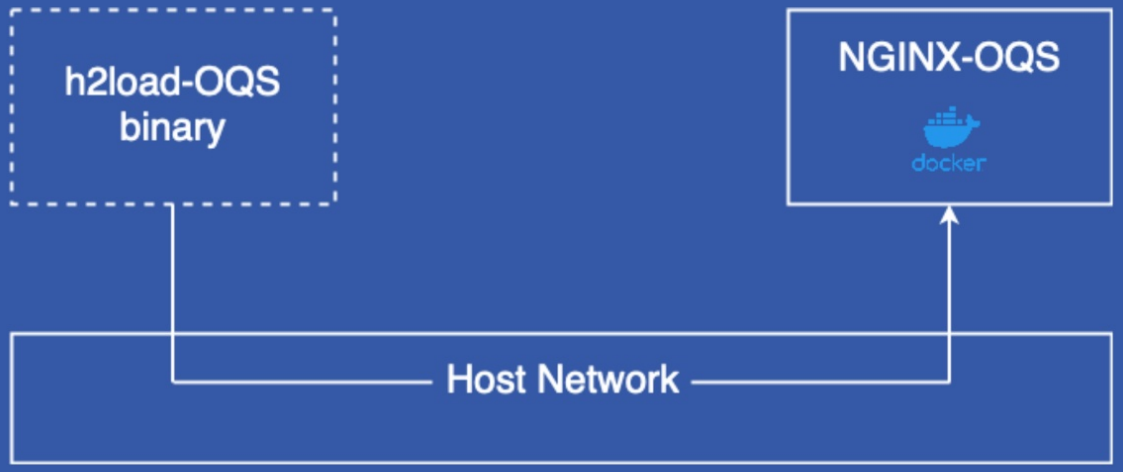
Enter Email Address

Literature Performance

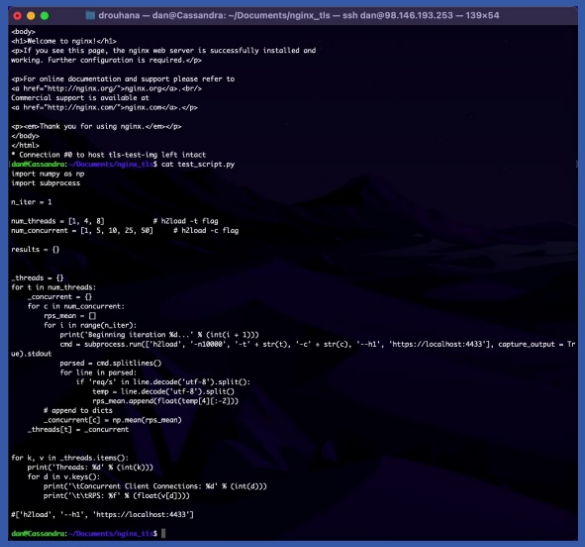


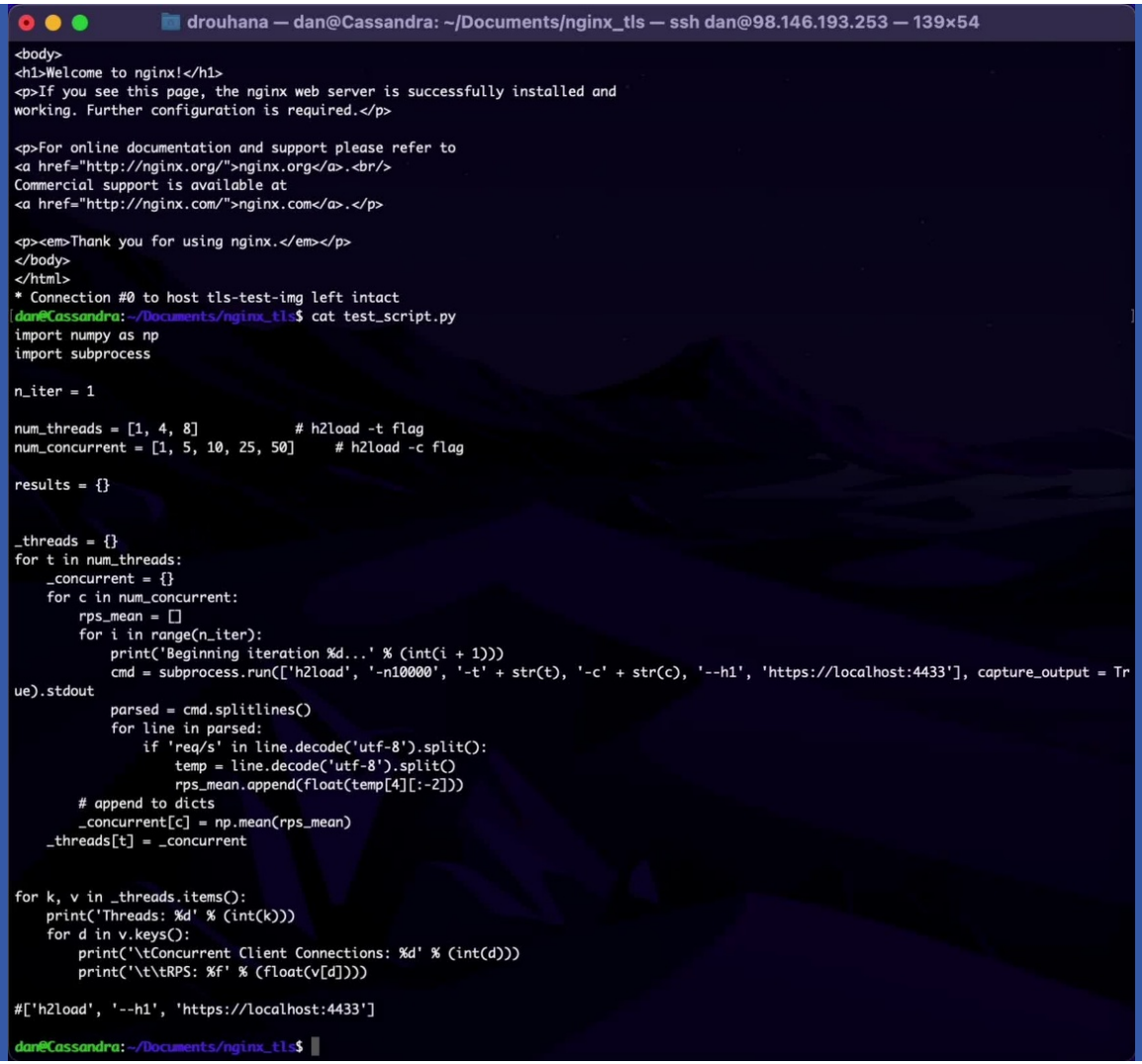
"Post-Quantum Authentication in TLS 1.3: A Performance Study", Sikeridis (2020)

NGINX Benchmarking

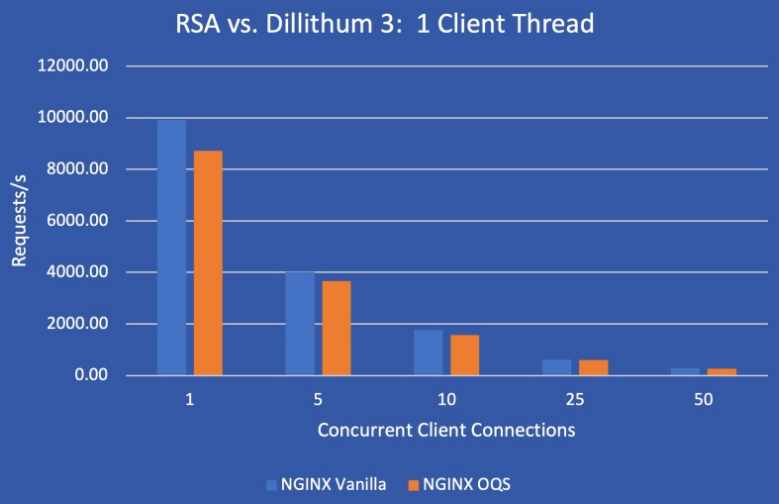


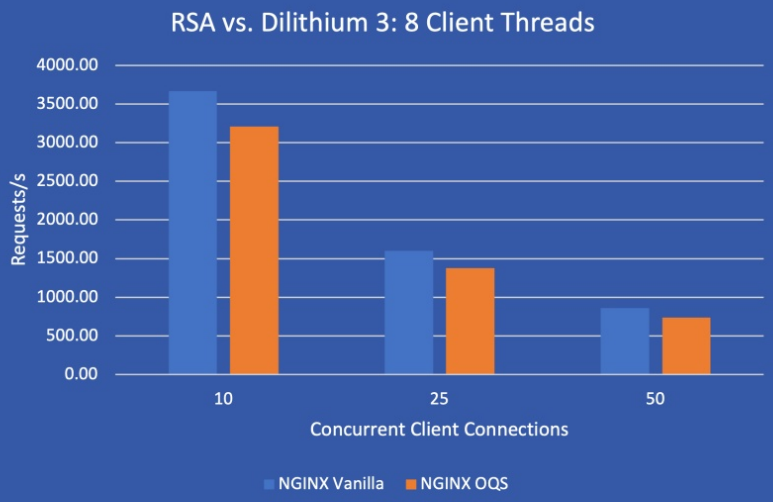
NGINX Benchmarking Demo



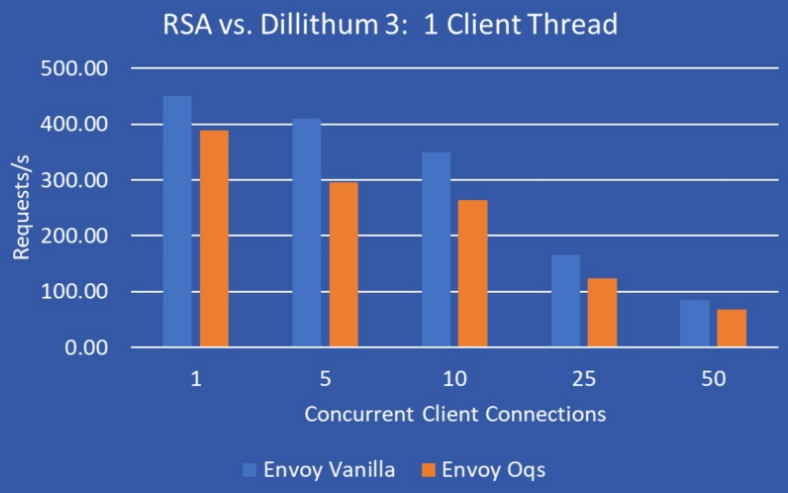

drouhana — dan@Cassandra: ~/Documents/nginx_tls — ssh dan@98.146.193.253 — 139×54
<body>
<h1>Welcome to nginx!</h1>
If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.
For online documentation and support please refer to
nginx.org.
Commercial support is available at
nginx.com.
Thank you for using nginx.
</body>
</html>
* Connection #0 to host tls-test-img left intact
dan@Cassandra:~/Documents/nginx_tls$ cat test_script.py
import numpy as np
import subprocess
n_iter = 1
num_threads = [1, 4, 8] # h2load -t flag
num_concurrent = [1, 5, 10, 25, 50] # h2load -c flag
results = {}
_threads = {}
for t in num_threads:
_concurrent = {}
for c in num_concurrent:
rps_mean = []
for i in range(n_iter):
print('Beginning iteration %d...' % (int(i + 1)))
cmd = subprocess.run(['h2load', '-n10000', '-t' + str(t), '-c' + str(c), '--h1', 'https://localhost:4433'], capture_output = Tr
ue).stdout
parsed = cmd.splitlines()
for line in parsed:
if 'req/s' in line.decode('utf-8').split():
temp = line.decode('utf-8').split()
rps_mean.append(float(temp[4][:-2]))
# append to dicts
_concurrent[c] = np.mean(rps_mean)
_threads[t] = _concurrent
for k, v in _threads.items():
print('Threads: %d' % (int(k)))
for d in v.keys():
print('\tConcurrent Client Connections: %d' % (int(d)))
print('\t\tRPS: %f' % (float(v[d])))
#['h2load', '--h1', 'https://localhost:4433']
dan@Cassandra:~/Documents/nginx_tls$

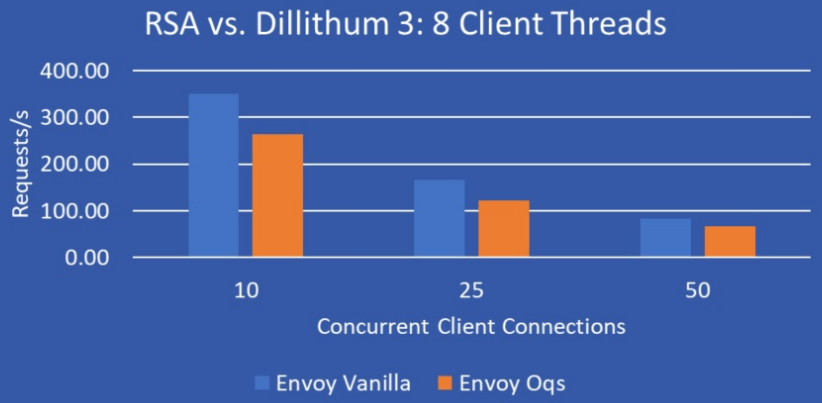
NGINX Performance





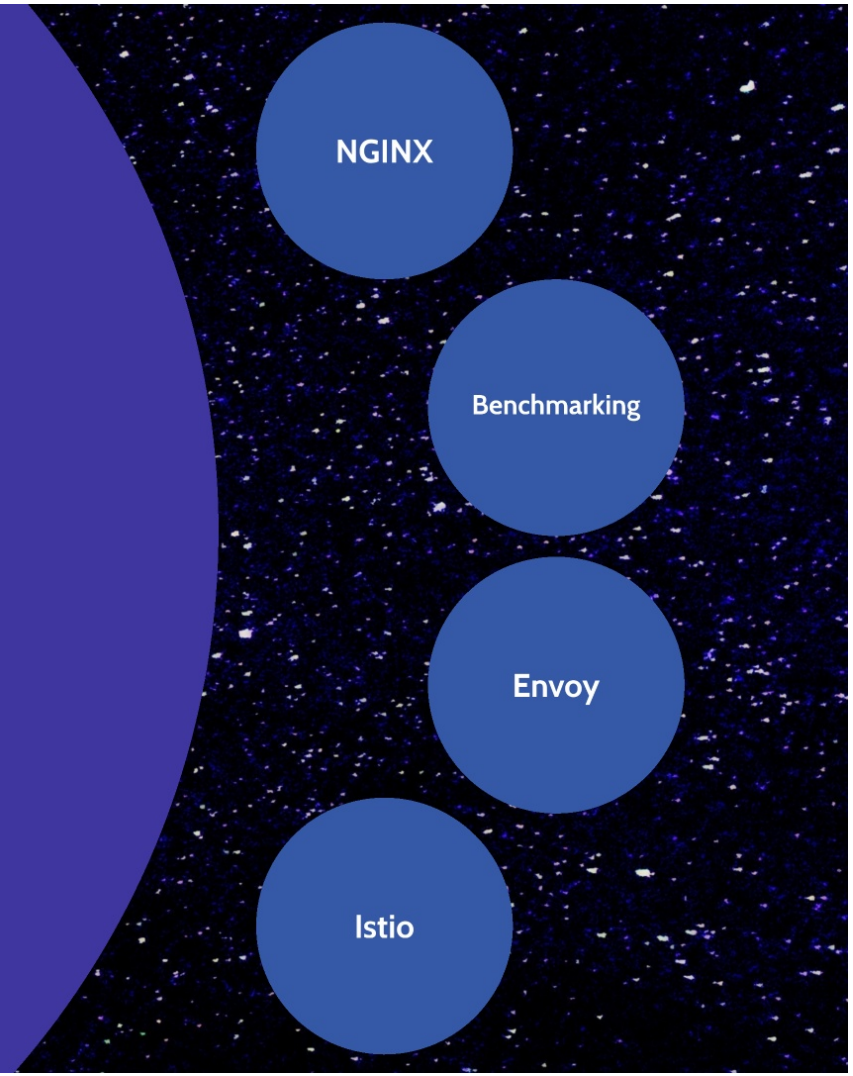
Envoy Performance





Post-Quantum Stack

- OpenQuantumSafe library
- NGINX v1.20
- Envoy v1.23.1
- Istio v1.25
- Kubernetes v1.25
- Minikube v1.27
- BoringSSL-OQS



High performance server
- Small footprint

Cloud and cloud-native application hosting

Solves specific challenges:
- Maintaining network in heterogenous systems
- Difficulty in monitoring traffic
- Scaling microservices

Development

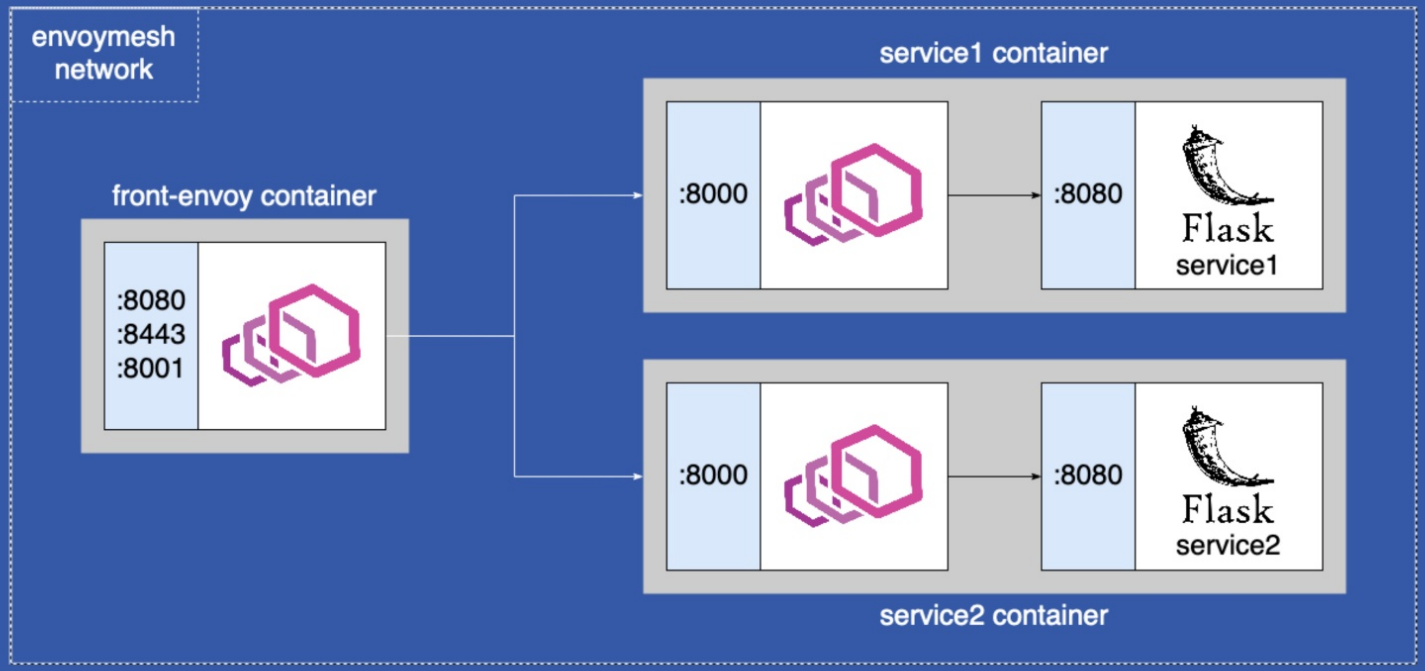
BoringSSL development

- Updated to most recent source code (3f56764)
- Bazel build dependencies (842e9c0)
- Makefile targets (be0722d)

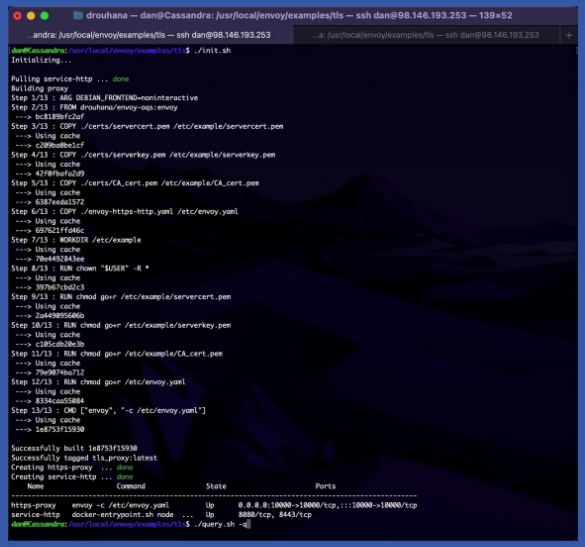
Envoy porting

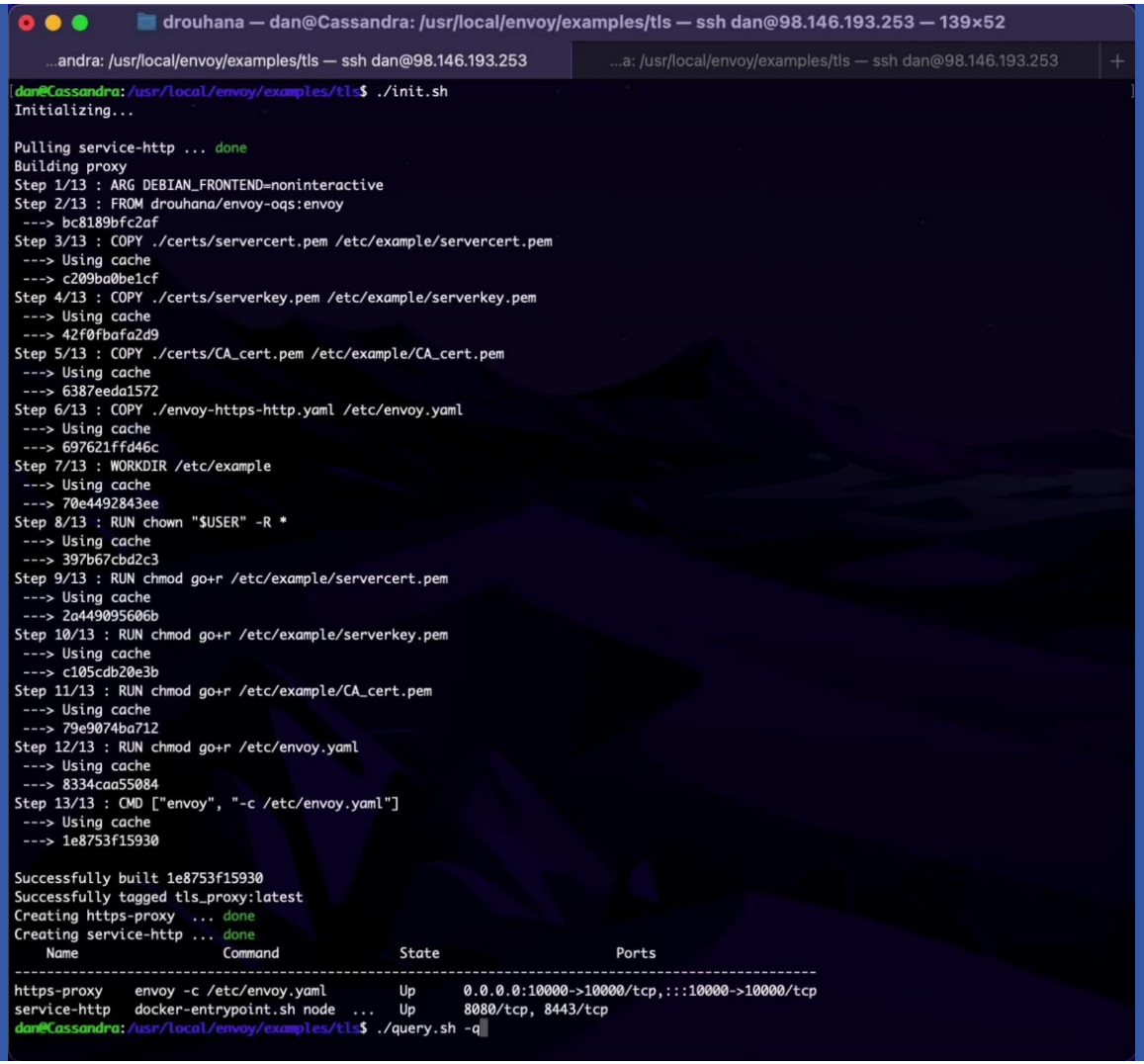
- Updated boringssl targets and dependencies (a5c053d)

Front-Proxy Sample Architecture

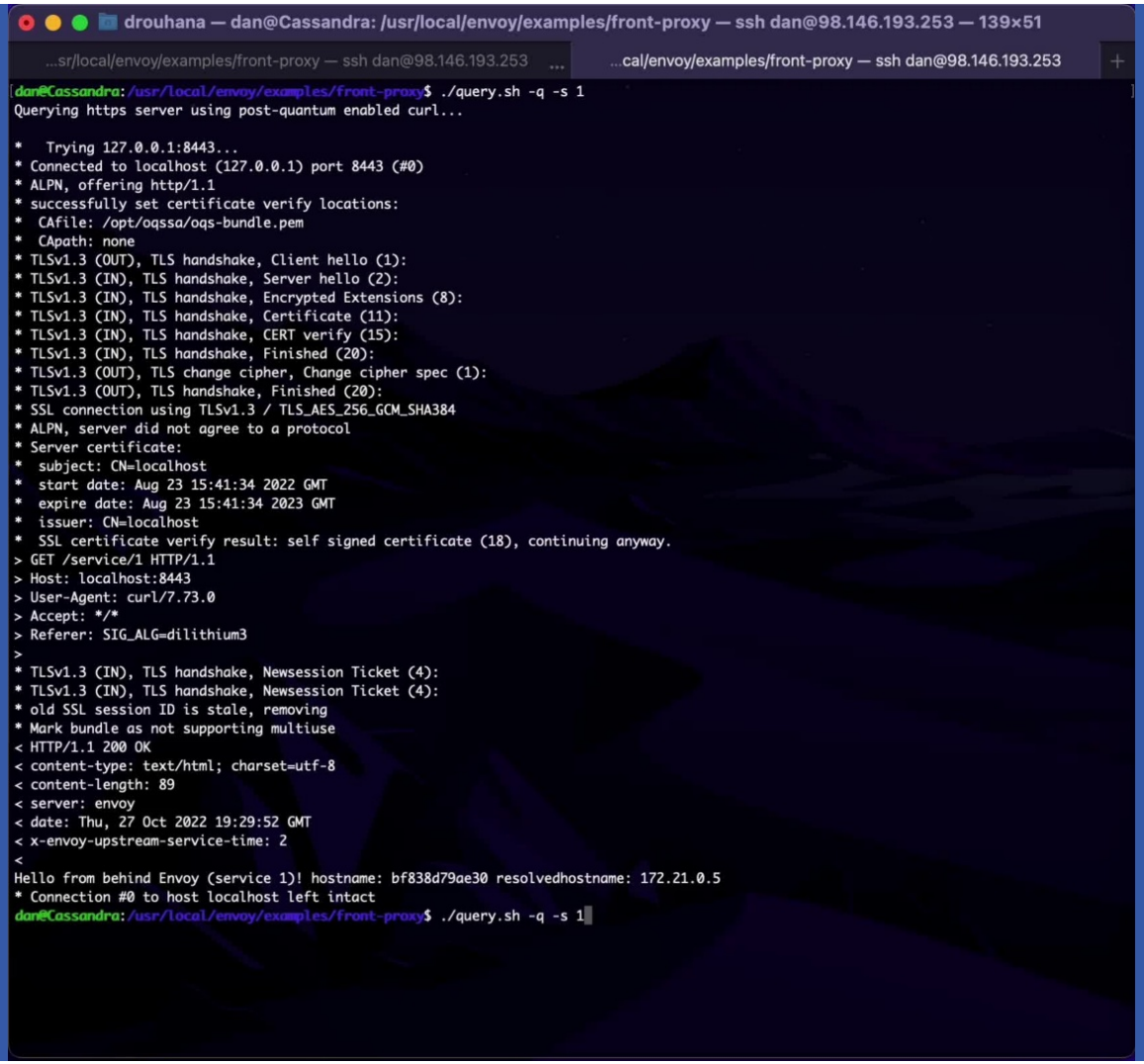


TLS Demo


drouhana — dan@Cassandra: /usr/local/envoy/examples/tls — ssh dan@98.146.193.253 — 139×52
./init.sh
Initializing...
Pulling service-http ... done
Building proxy
Step 1/13 : ARG DEBIAN_FRONTEND=noninteractive
Step 2/13 : FROM drouhana/envoy-ops:envoy
Step 3/13 : COPY ./certs/servercert.pem /etc/example/servercert.pem
Step 4/13 : COPY ./certs/serverkey.pem /etc/example/serverkey.pem
Step 5/13 : COPY ./certs/CA_cert.pem /etc/example/CA_cert.pem
Step 6/13 : COPY ./envoy-https-http.yaml /etc/envoy.yaml
Step 7/13 : WORKDIR /etc/example
Step 8/13 : RUN chown "$USER" -R *
Step 9/13 : RUN chmod go+r /etc/example/servercert.pem
Step 10/13 : RUN chmod go+r /etc/example/serverkey.pem
Step 11/13 : RUN chmod go+r /etc/example/CA_cert.pem
Step 12/13 : RUN chmod go+r /etc/envoy.yaml
Step 13/13 : CMD ["envoy", "-c /etc/envoy.yaml"]
Successfully built 1e8753f15930
Successfully tagged tls_proxy:latest
Creating https-proxy ... done
Creating service-http ... done
Name Command State Ports
https-proxy envoy -c /etc/envoy.yaml Up 0.0.0.0:10000->10000/tcp,:::10000->10000/tcp
service-http docker-entrypoint.sh node ... Up 8888/tcp, 8443/tcp
./query.sh -c

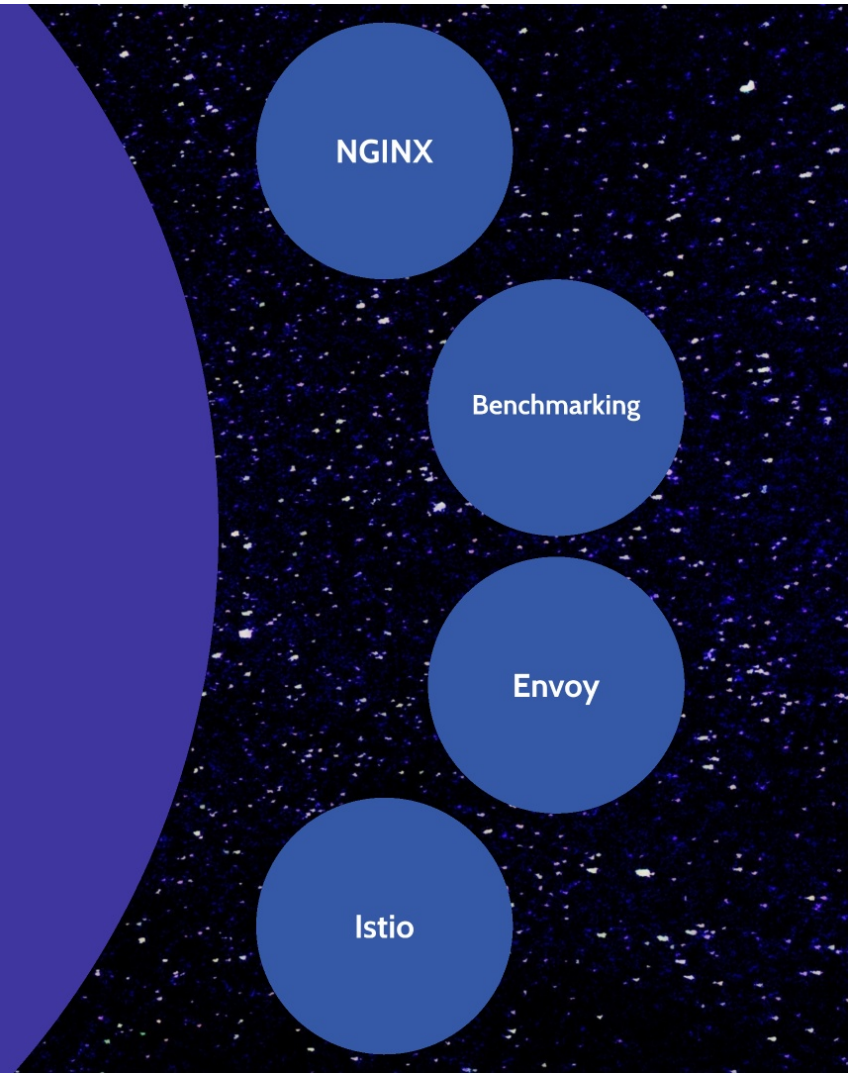

drouhana — dan@Cassandra: /usr/local/envoy/examples/tls — ssh dan@98.146.193.253 — 139×52
...andra: /usr/local/envoy/examples/tls — ssh dan@98.146.193.253
...a: /usr/local/envoy/examples/tls — ssh dan@98.146.193.253
dan@Cassandra:/usr/local/envoy/examples/tls$ ./init.sh
Initializing...
Pulling service-http ... done
Building proxy
Step 1/13 : ARG DEBIAN_FRONTEND=noninteractive
Step 2/13 : FROM drouhana/envoy-oqs:envoy
---> bc8189bfc2af
Step 3/13 : COPY ./certs/servercert.pem /etc/example/servercert.pem
---> Using cache
---> c209ba0be1cf
Step 4/13 : COPY ./certs/serverkey.pem /etc/example/serverkey.pem
---> Using cache
---> 42f0fbafa2d9
Step 5/13 : COPY ./certs/CA_cert.pem /etc/example/CA_cert.pem
---> Using cache
---> 6387eeda1572
Step 6/13 : COPY ./envoy-https-http.yaml /etc/envoy.yaml
---> Using cache
---> 697621ffd46c
Step 7/13 : WORKDIR /etc/example
---> Using cache
---> 70e4492843ee
Step 8/13 : RUN chown "$USER" -R *
---> Using cache
---> 397b67cbd2c3
Step 9/13 : RUN chmod go+r /etc/example/servercert.pem
---> Using cache
---> 2a449095606b
Step 10/13 : RUN chmod go+r /etc/example/serverkey.pem
---> Using cache
---> c105cdb20e3b
Step 11/13 : RUN chmod go+r /etc/example/CA_cert.pem
---> Using cache
---> 79e9074ba712
Step 12/13 : RUN chmod go+r /etc/envoy.yaml
---> Using cache
---> 8334caa55084
Step 13/13 : CMD ["envoy", "-c /etc/envoy.yaml"]
---> Using cache
---> 1e8753f15930
Successfully built 1e8753f15930
Successfully tagged tls_proxy:latest
Creating https-proxy ... done
Creating service-http ... done
Name Command State Ports
https-proxy envoy -c /etc/envoy.yaml Up 0.0.0.0:10000->10000/tcp,:::10000->10000/tcp
service-http docker-entrypoint.sh node ... Up 8080/tcp, 8443/tcp
dan@Cassandra:/usr/local/envoy/examples/tls$ ./query.sh -q

Front-Proxy Demo


drouhana — dan@Cassandra: /usr/local/envoy/examples/front-proxy — ssh dan@98.146.193.253 — 139×51
...sr/local/envoy/examples/front-proxy — ssh dan@98.146.193.253
...cal/envoy/examples/front-proxy — ssh dan@98.146.193.253
dan@Cassandra:/usr/local/envoy/examples/front-proxy$ ./query.sh -q -s 1
Querying https server using post-quantum enabled curl...
*   Trying 127.0.0.1:8443...
* Connected to localhost (127.0.0.1) port 8443 (#0)
* ALPN, offering http/1.1
* successfully set certificate verify locations:
* CAfile: /opt/oqssa/oqs-bundle.pem
* CApath: none
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server did not agree to a protocol
* Server certificate:
* subject: CN=localhost
* start date: Aug 23 15:41:34 2022 GMT
* expire date: Aug 23 15:41:34 2023 GMT
* issuer: CN=localhost
* SSL certificate verify result: self signed certificate (18), continuing anyway.
> GET /service/1 HTTP/1.1
> Host: localhost:8443
> User-Agent: curl/7.73.0
> Accept: */*
> Referer: SIG_ALG=dilithium3
>
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* old SSL session ID is stale, removing
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< content-type: text/html; charset=utf-8
< content-length: 89
< server: envoy
< date: Thu, 27 Oct 2022 19:29:52 GMT
< x-envoy-upstream-service-time: 2
<
Hello from behind Envoy (service 1)! hostname: bf838d79ae30 resolvedhostname: 172.21.0.5
* Connection #0 to host localhost left intact
dan@Cassandra:/usr/local/envoy/examples/front-proxy$ ./query.sh -q -s 1

Post-Quantum Stack

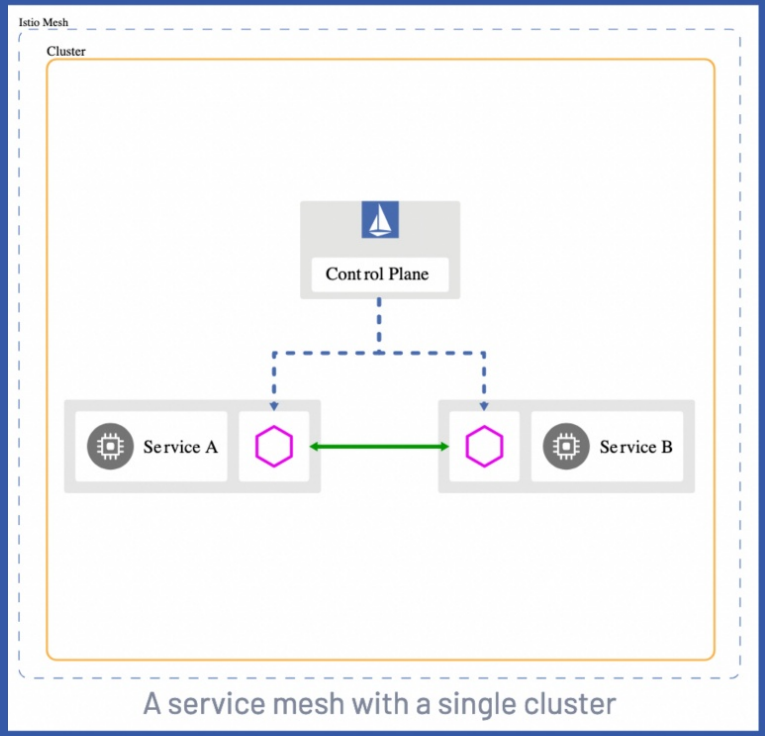
- OpenQuantumSafe library
- NGINX v1.20
- Envoy v1.23.1
- Istio v1.25
- Kubernetes v1.25
- Minikube v1.27
- BoringSSL-OQS



Istio

Multi-modal open platform

- Microservice integration
- Traffic flow management
- Policy enforcement



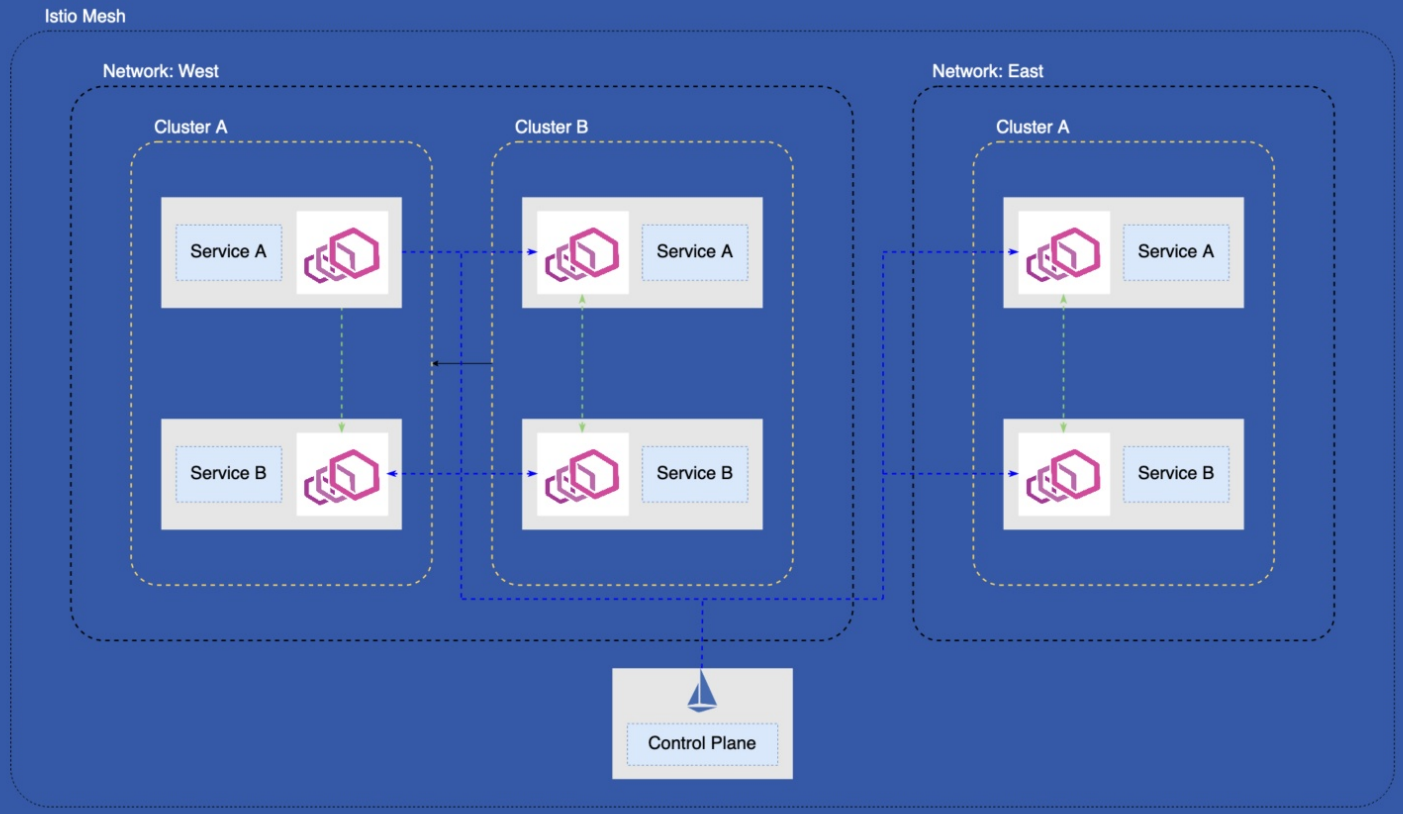
A service mesh with a single cluster

Development

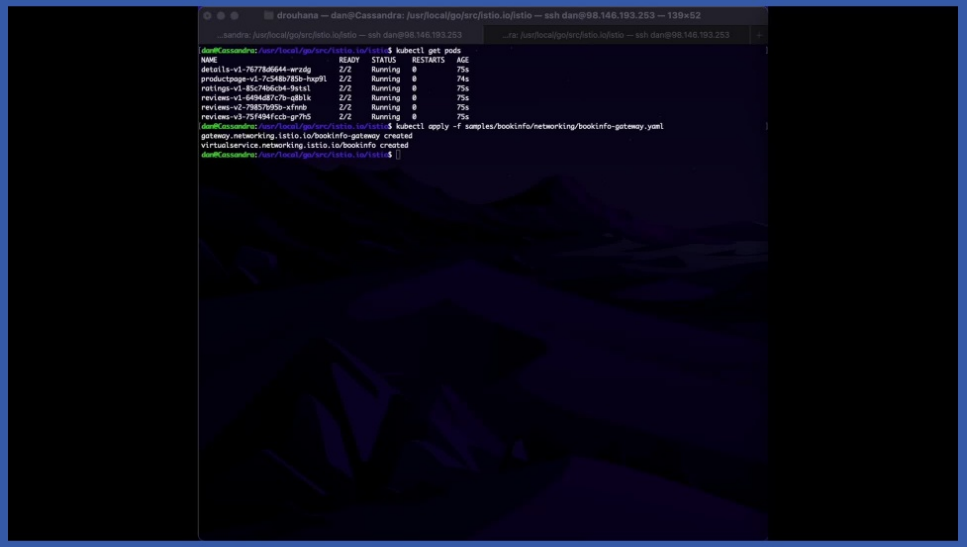
Istio porting
- No source code modification
- Update repository targets (5c81192)

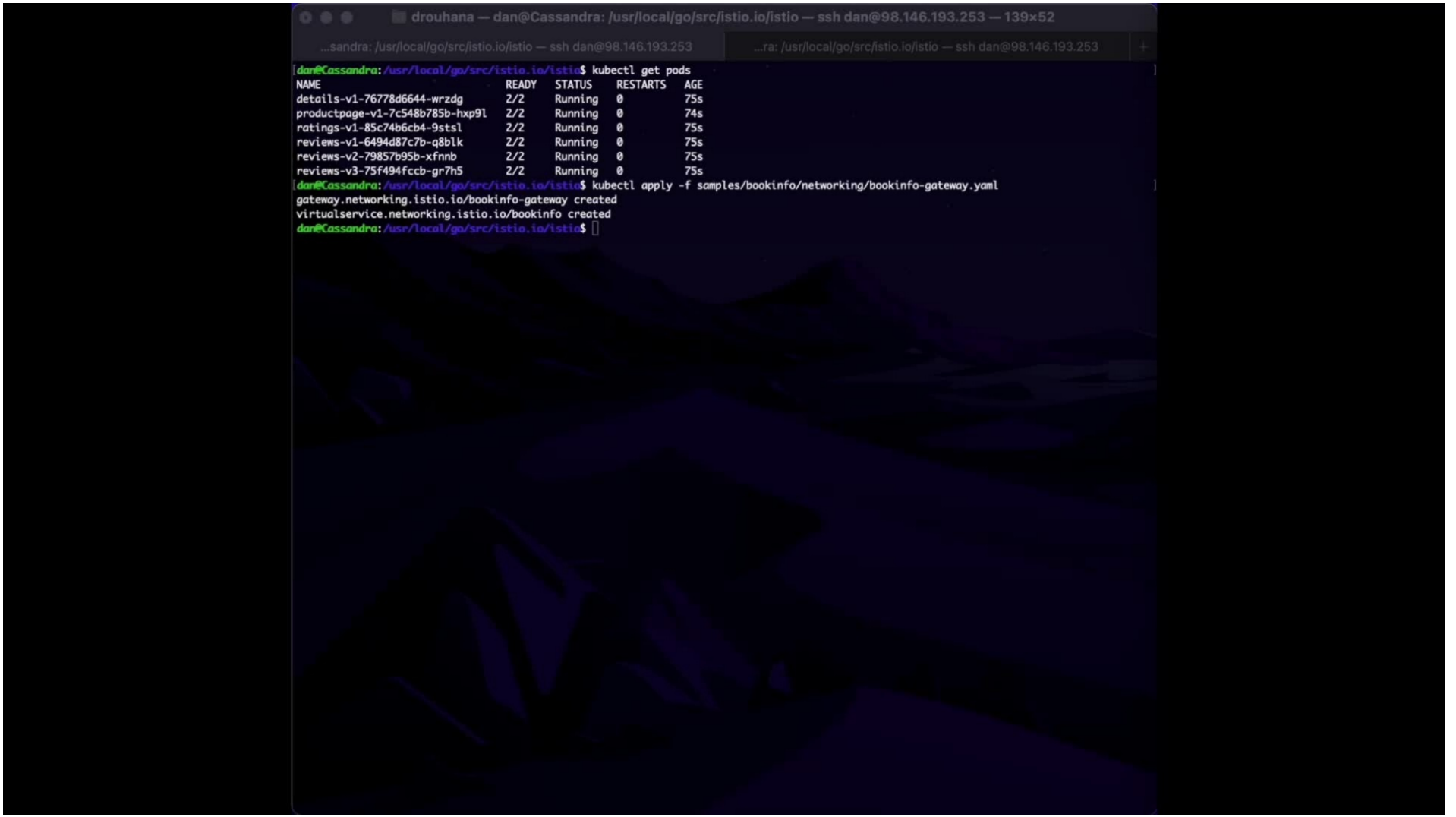
Build process
- Make istio/proxy against Envoy image
- Make istio/istio with modified proxy

Why Istio?


Istio Mesh
Network: West
Cluster A
Service A
Service B
Cluster B
Service A
Service B
Network: East
Cluster A
Service A
Service B
Control Plane

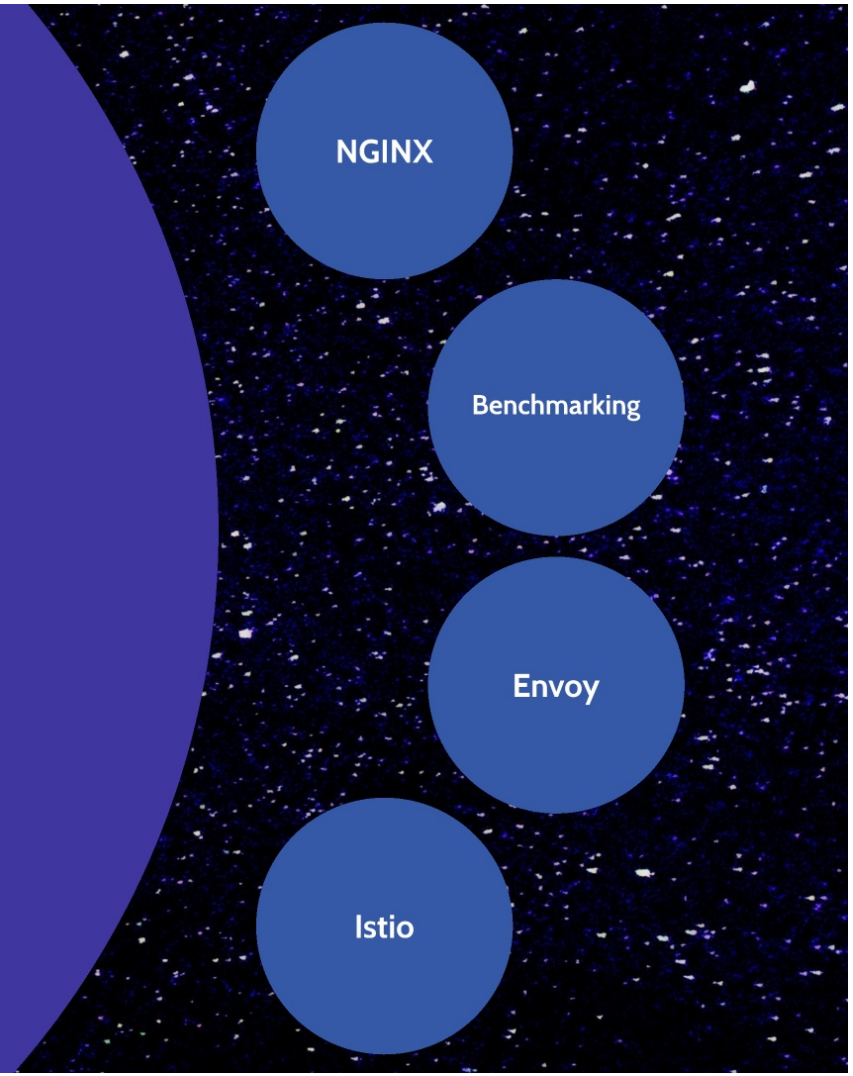
Istio BookInfo Demo

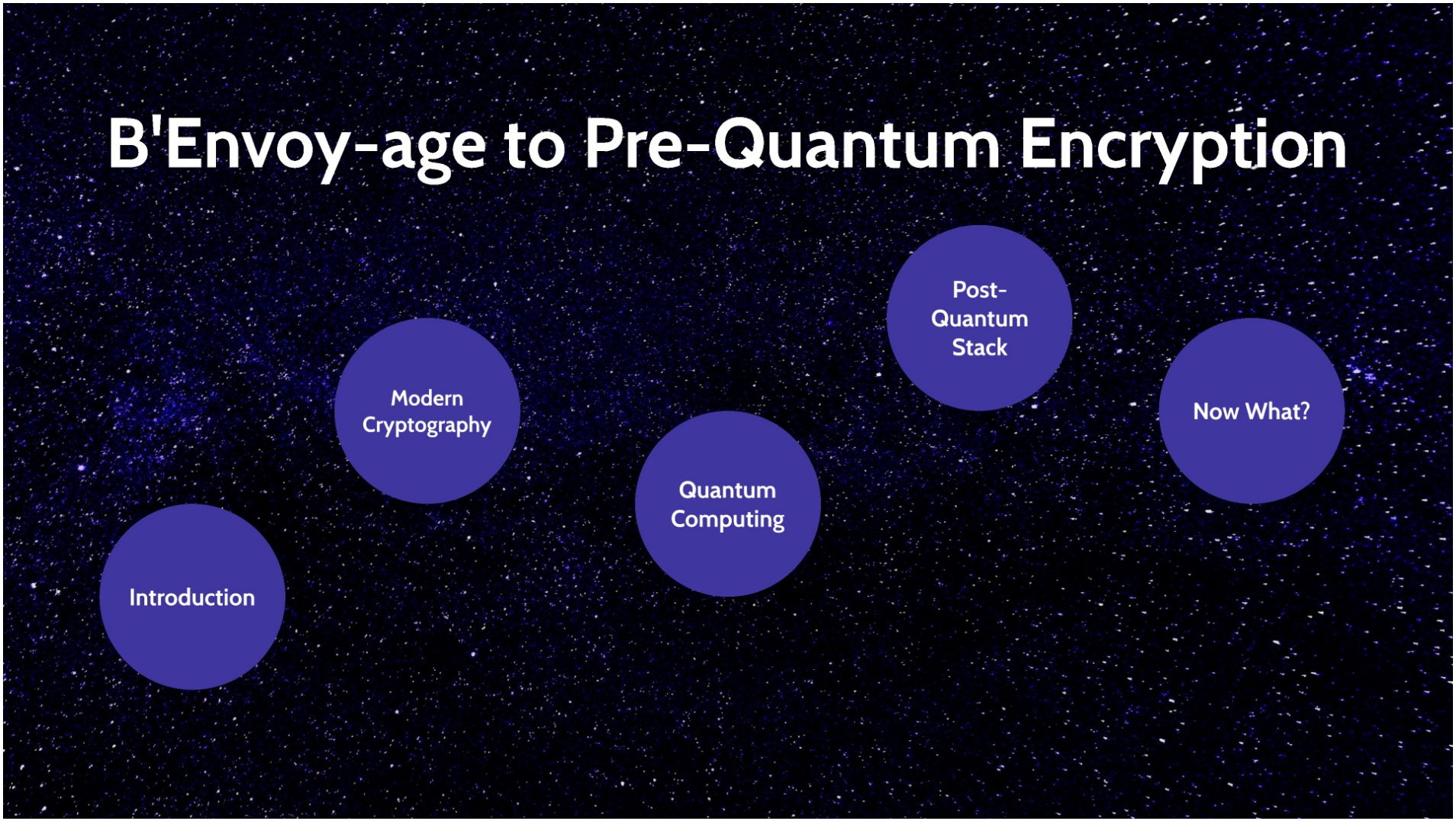



drouhana — dan@Cassandra: /usr/local/go/src/istio.io/istio — ssh dan@98.146.193.253 — 139×52
...sandra: /usr/local/go/src/istio.io/istio — ssh dan@98.146.193.253
...ra: /usr/local/go/src/istio.io/istio — ssh dan@98.146.193.253
dan@Cassandra: /usr/local/go/src/istio.io/istio$ kubectl get pods
NAME READY STATUS RESTARTS AGE
details-v1-76778d6644-wrzdg 2/2 Running 0 75s
productpage-v1-7c548b785b-hxp9l 2/2 Running 0 74s
ratings-v1-85c74b6cb4-9stsl 2/2 Running 0 75s
reviews-v1-6494d87c7b-q8blk 2/2 Running 0 75s
reviews-v2-79857b95b-xfnnb 2/2 Running 0 75s
reviews-v3-75f494fccb-gr7h5 2/2 Running 0 75s
dan@Cassandra: /usr/local/go/src/istio.io/istio$ kubectl apply -f samples/bookinfo/networking/bookinfo-gateway.yaml
gateway.networking.istio.io/bookinfo-gateway created
virtualservice.networking.istio.io/bookinfo created
dan@Cassandra: /usr/local/go/src/istio.io/istio$

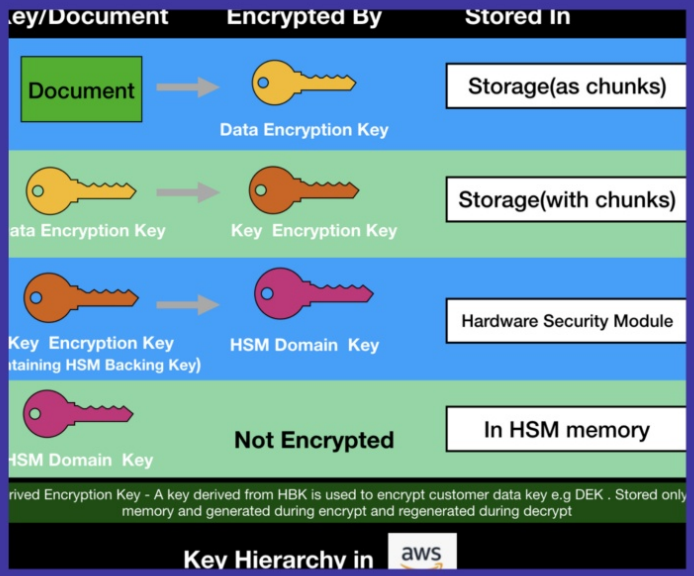
Post-Quantum Stack

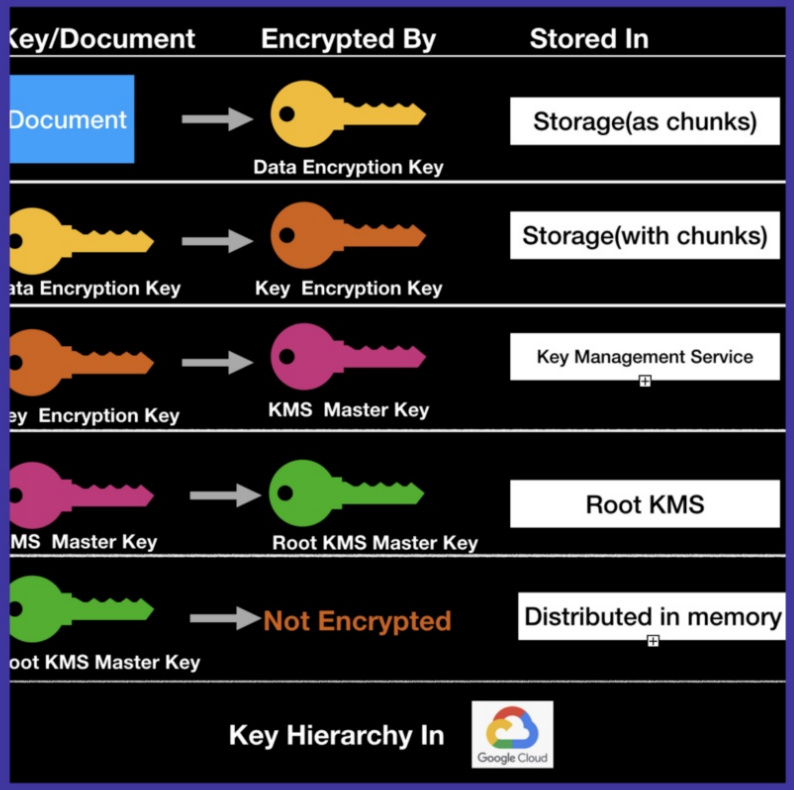
- OpenQuantumSafe library
- NGINX v1.20
- Envoy v1.23.1
- Istio v1.25
- Kubernetes v1.25
- Minikube v1.27
- BoringSSL-OQS



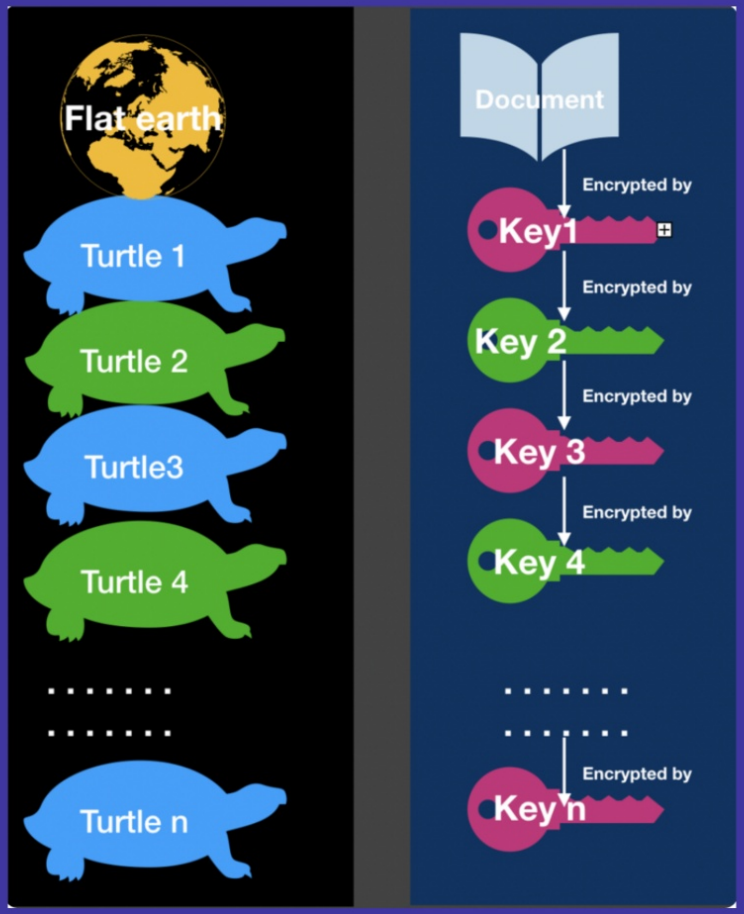

B'Envoy-age to Pre-Quantum Encryption
Introduction
Modern Cryptography
Quantum Computing
Post-Quantum Stack
Now What?

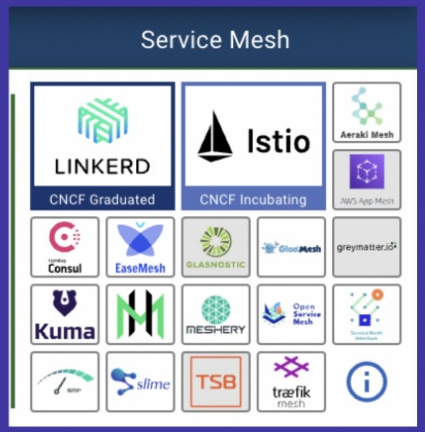
Now What?

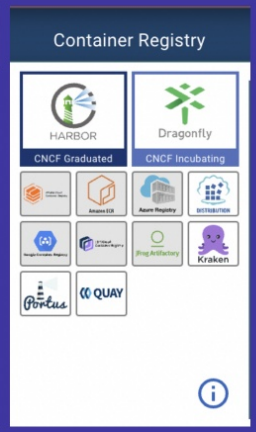




https://www.linkedin.com/pulse/key-hierarchy-cloud-turtles-all-way-down-pragyan-mishra/


Flat earth
Turtle 1
Turtle 2
Turtle3
Turtle 4
Turtle n
Document
Encrypted by
Key1
Encrypted by
Key 2
Encrypted by
Key 3
Encrypted by
Key 4
Encrypted by
Key n


Service Mesh
LINKERD
CNCF Graduated
Istio
CNCF Incubating
Aeraki Mesh
AWS App Mesh
Consul
EaseMesh
GLASNOSTIC
GlooMesh
greymatter.io
Kuma
MESHERY
Open Service Mesh
SlimeMesh Interface
slime
TSB
træfik mesh


Container Registry
HARBOR
CNCF Graduated
Dragonfly
CNCF Incubating
Amazon ECR
Azure Registry
DISTRIBUTION
Google Container Registry
Virtual Kubelet Azure Batch
JFrog Artifactory
Kraken
Portus
QUAY


Key Management
spiffe
CNCF Graduated
SPIRE
CNCF Graduated
Athenz
Authing
CYBERARK CONJUR
KEYCLOAK
OAuth2 Proxy
ORY / Hydra
PINNIPED
POMERIUM
Square Keywhiz
sso
Teleport
teller
Vault


Security & Compliance
Open Policy Agent
CNCF Graduated
TUF
CNCF Graduated
CNCF Incubating
falco
CNCF Incubating
in-toto
CNCF Incubating
Kyverno
CNCF Incubating
notary
CNCF Incubating
AIRLOCK
alcide
anchore
apolicy
aqua
ARMO
BLACK DUCK
Bloombase
CAPSULE8
cerbos
Check Point
checkov
CHEF INSPEC
clair
CONFIDENTIAL CONTAINERS
ContainerSSH
Curiefense
Datica
datree
dex
DOSEC
Fairwinds Insights
FOSSA
FOSSID
Fugue
Goldilocks
Grafeas
Hexa
Keylime
kics
kube-bench
kube-hunter
kubearmor
KUBEWARDEN
mondoo
NeuVector
nirmata
OpenFGA
OpenSCAP
orca security
oxeye
PALADIN
PARSEC
Passage
pluto
polaris
portshift
PRISMA CLOUD
RBAC LOOKUP
rbac manager
Rudder
scribe
sigstore
snyk
nexus repository
SONOBUOY
SYNOPSYS
STACKHAWK
StackRox
starboard
sysdig
terrascan
Tetragon
ThreatMapper
TIGERA
TREND MICRO
trivy
WhiteSource
Zettaset

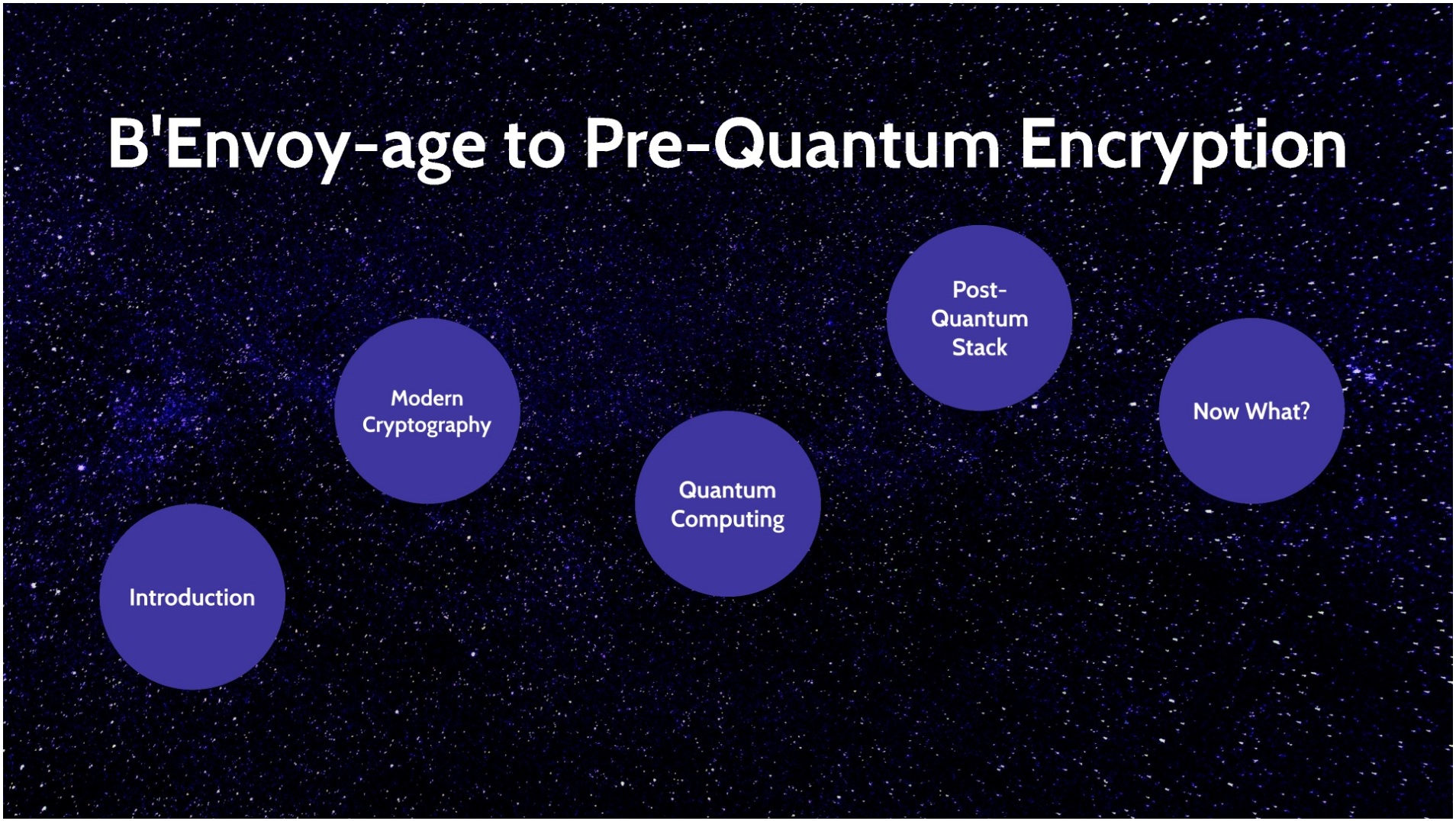
Github Repository

Feedback

Special thanks to:

Aron Wahl, whose technical consultation made this possible.

Christian Rouhana, for the unlimited access to compute.


B'Envoy-age to Pre-Quantum Encryption
Introduction
Modern Cryptography
Quantum Computing
Post-Quantum Stack
Now What?