Google | Privacy, Safety & Security

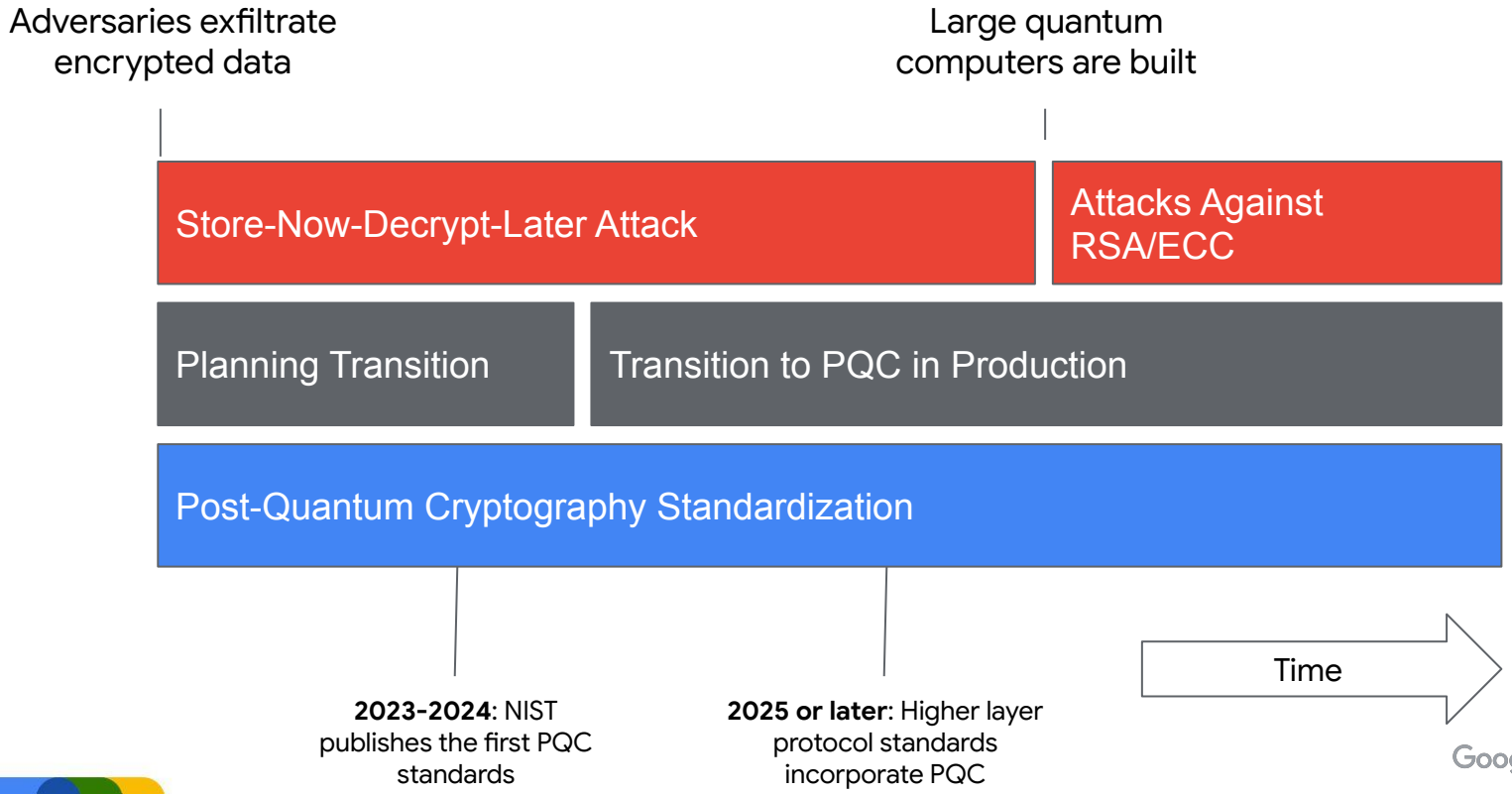
# Post-Quantum Cryptography at Google

**Sophie Schmieg**

IETF 117

July 25th, 2023

# Why is this important now?



# PQC Priorities

1) Encryption in Transit
2) Signatures, when Public Keys are hard to change
3) All other Asymmetric Cryptography
4) Symmetric Cryptography (in case we get bored)

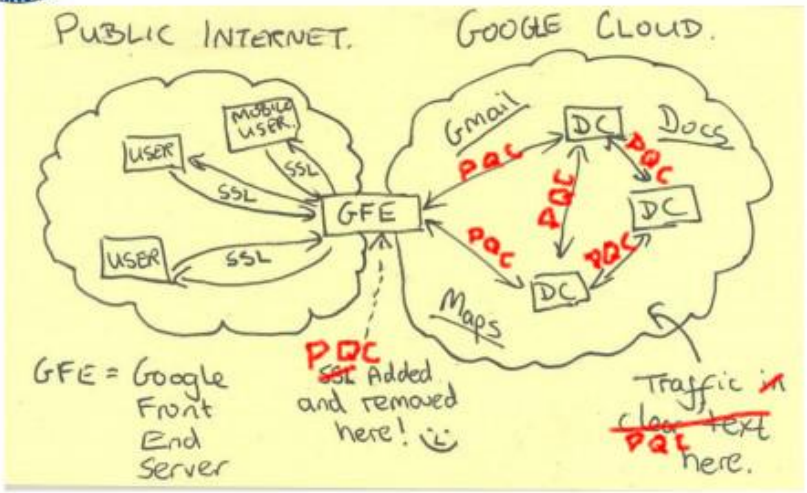
# The PQC Kitchen Sink Problem

1) Hybridization multiplies ciphersuites
2) Each ciphersuite should have a clear role
3) Implementation complexity

# PQC ALTS: Overview

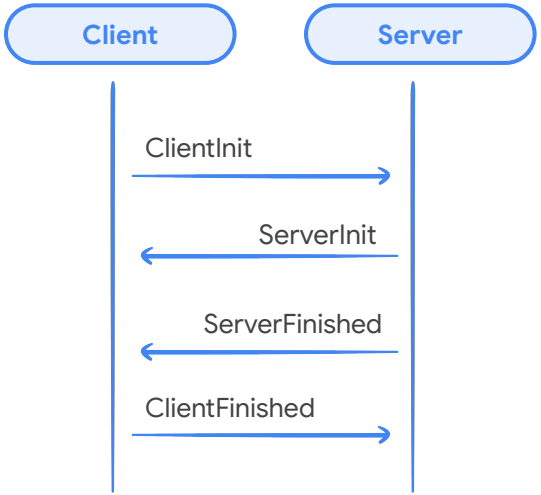
TOP SECRET//SI//NOFORN

## Current Efforts - Google




TOP SECRET//SI//NOFORN

# ALTS: Overview




**ClientInit**

- static ECDH key
- cert for ECDH key

**ServerInit**

- static ECDH key
- cert for ECDH key

**ServerFinished**

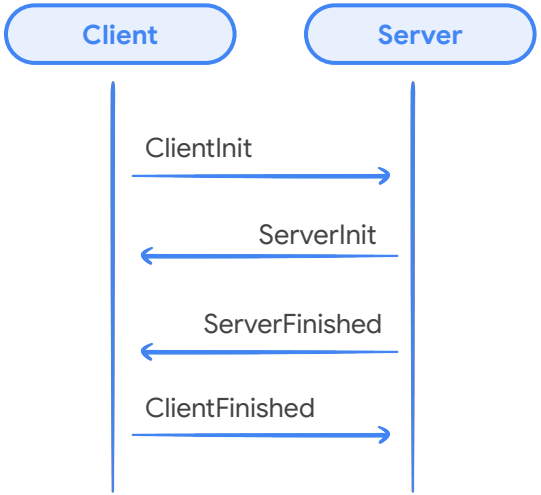
- HMAC(shared_secret, server_const)

**ClientFinished**

- HMAC(shared_secret, client_const)

Documentation: https://cloud.google.com/docs/security/encryption-in-transit/application-layer-transport-security

# ALTS: Overview




**ClientInit**

- static ECDH key
- cert for ECDH key
- resumption ticket

**ServerInit**

- resumption confirmation

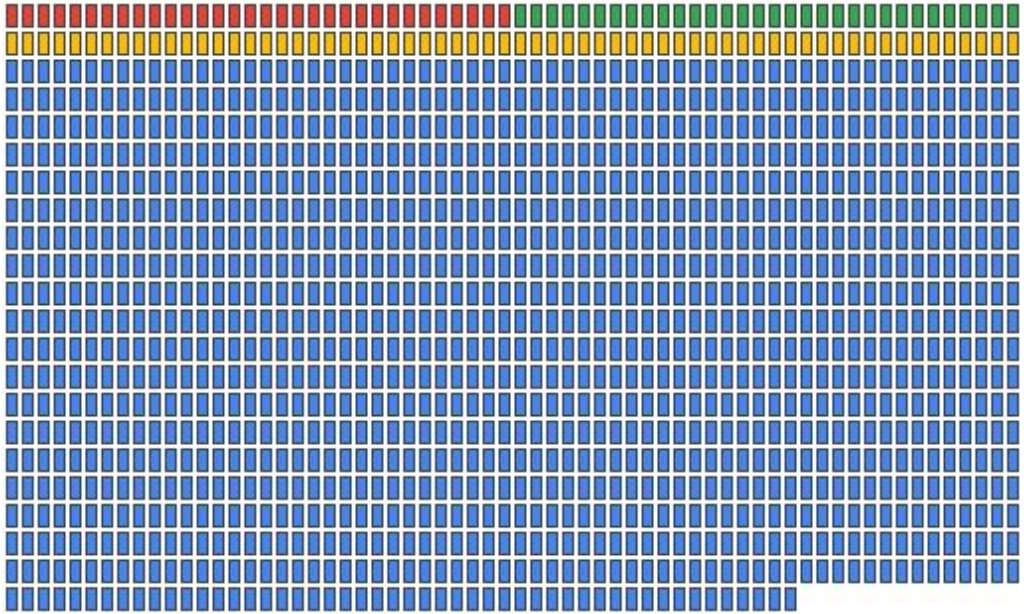
**ServerFinished**

- HMAC(shared_secret, server_const)

**ClientFinished**

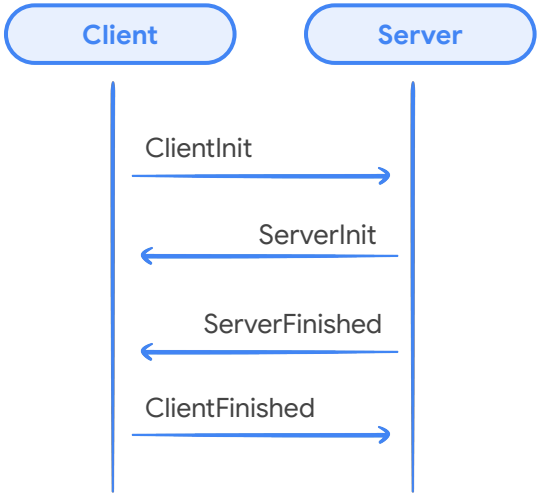
- HMAC(shared_secret, client_const)

# PQC Overview



- Protocol Overhead (estimate)
- X25519 Keyshare
- Certificate
- HRSS public key/ciphertext

# ALTS PQC




**ClientInit**

- static ECDH key
- cert for ECDH key
- ephemeral PQC public key

**ServerInit**

- static ECDH key
- cert for ECDH key
- PQC KEM ciphertext

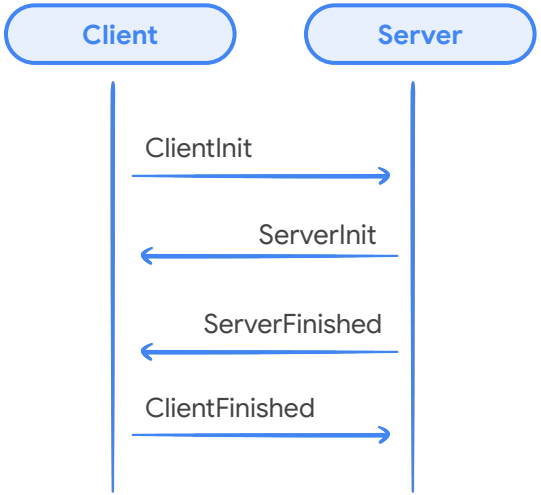
**ServerFinished**

- HMAC(shared_secret, server_const)

**ClientFinished**

- HMAC(shared_secret, client_const)

# ALTS PQC




**ClientInit**

- static ECDH key
- cert for ECDH key
- somewhat ephemeral PQC public key

**ServerInit**

- static ECDH key
- cert for ECDH key
- PQC KEM ciphertext

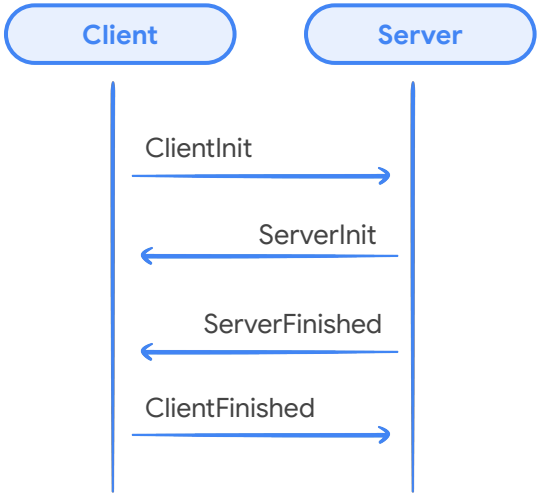
**ServerFinished**

- HMAC(shared_secret, server_const)

**ClientFinished**

- HMAC(shared_secret, client_const)

# ALTS PQC




**ClientInit**

- static ECDH key
- cert for ECDH key
- resumption ticket
- somewhat ephemeral PQC public key

**ServerInit**

- resumption confirmation
- PQC KEM ciphertext

**ServerFinished**

- HMAC(shared_secret, server_const)

**ClientFinished**

- HMAC(shared_secret, client_const)

# Takeaways

01

## Threat Modelling PQC

Encryption in transit, as well as hardware roots of trust are the highest priorities and it can be argued that migration in these cases needs to start as soon as possible

02

## Hybrid deployment

Hybrid deployment allows us to experiment with PQC without risking security regressions. In the worst case, we learned something in an experiment, in the best case we have already mitigated store-now-decrypt later

03

## Rolling out PQC

We started working on ALTS PQC in 2020, and are now finally getting ready to have rolled out PQC for all jobs, with many unforeseen obstacles along the way.

# Thank you