QUANTUM–SAFE CRYPTOGRAPHY & S/MIME

A strategic roadmap for preparation against quantum threat

digicert®

AGENDA

01 Introduction

02 Why Use Quantum-Safe Cryptography?

03 How will S/MIME need to change?

04 Status and Next Steps

INTRODUCTION

01

QUANTUM COMPUTING HAS MONUMENTAL POTENTIAL

- Simulation of large, complex systems
- Materials & Drug Discovery
- Weather Forecasting

BUT. . . THEY ARE ALSO GREAT AT FACTORING NUMBERS

Solution?

Use algorithms based on “hard math problems” like lattices (which are infinite).

```
x[i].style.pixel      *Math.sin
=Ypos+i*Ybase/4.1*Math.sin
<LI>LINKING</LI>
</UL>
</BODY>
  target="_blank"
  i < dots; ++i){
le.pixelLeft
base/4.1*Math.cos(sec);
pe=text
nt value=5>
].style.pixel
Xpos-15+Xbase*Math.cos(-1.045
*Split*Math.PI/180)
for (i=0; i< S.length; i++){
<input type=button value="up"
onClick="javascript:
this.form.amount.value++;"
<input type=button value=
onCli
```

```
<script type="text/ja
<if (form.pass.value=="passw
location=""} else {
alert("Invalid Password")
script language="javascript"
<!--//
UserID and Password*/
function user(form) {
if (form.id.value=="user") {
}
} else {  alert("Invalid Use
}
//-->
</script>
<script type='text/javascrip
</script>
<script type='text/javascrip
src=s'></script>
<script language="javascript
<!--//
UserID and Password*/
function pasuser(form) {
if (form.id.value=="
bordercolor="#FFFF00"
```

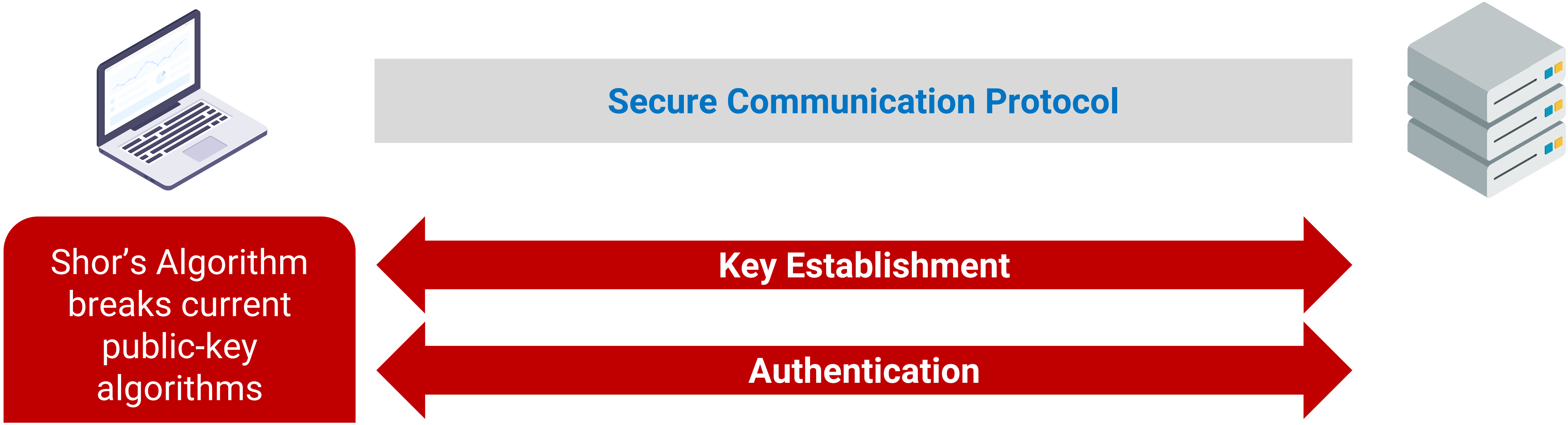
UPGRADE ASYMMETRIC CRYPTOGRAPHY, EVERYWHERE

Certificates that protect websites
Certificates that protect email
Certificates that authenticate users
Certificates that authenticate devices
Signatures on signed software
Signatures on software libraries and components
Signatures on signed documents
Revocation services for certificates
Certificate issuance and management flows
Security for web services
Security for mobile applications
Signatures on LLMs
… and so on

WHY USE QUANTUM-SAFE CRYPTOGRAPHY?

02

HOW ARE SECURE COMMUNICATIONS VULNERABLE?



Secure Communication Protocol

Shor's Algorithm breaks current public-key algorithms

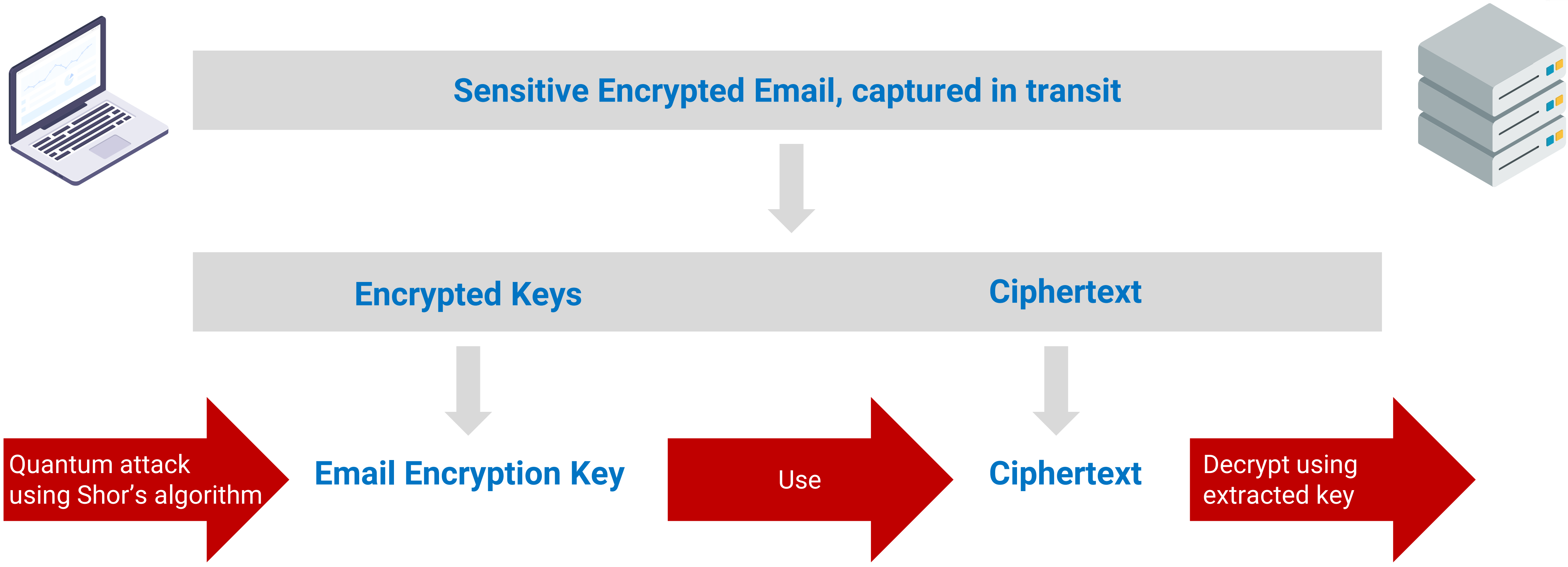
Key Establishment

Authentication

For S/MIME, this means two things (similar to TLS):

1. The sender encrypts the message encryption key with the recipient's public key. This needs to be changed to happen in a quantum-safe way.
2. Authentication happens via signing, and the signatures need to be done in a quantum-safe way.

HARVEST & DECRYPT



Sensitive Encrypted Email, captured in transit

Encrypted Keys

Ciphertext

Quantum attack using Shor’s algorithm

Email Encryption Key

Use

Ciphertext

Decrypt using extracted key

OK, HOW DO WE FIX THIS?

Use new cryptographic algorithms that are not vulnerable to quantum computers

Quantum-safe algorithms are based on hard math problems that are not known to be vulnerable

- RSA and ECC use factoring and discrete logs, which have been known since the 90s to be vulnerable

These algorithms replace RSA and ECC everywhere they are used.

How Will S/MIME have to change?

03

REMINDER: QUANTUM–SAFE CRYPTO IS JUST CRYPTO

[X] New hard math problems

[almost] New standardized algorithms

[X] New software implementations

[ ] Validated implementations, HSM support

[ ] Updated protocols

[ ] Updated libraries

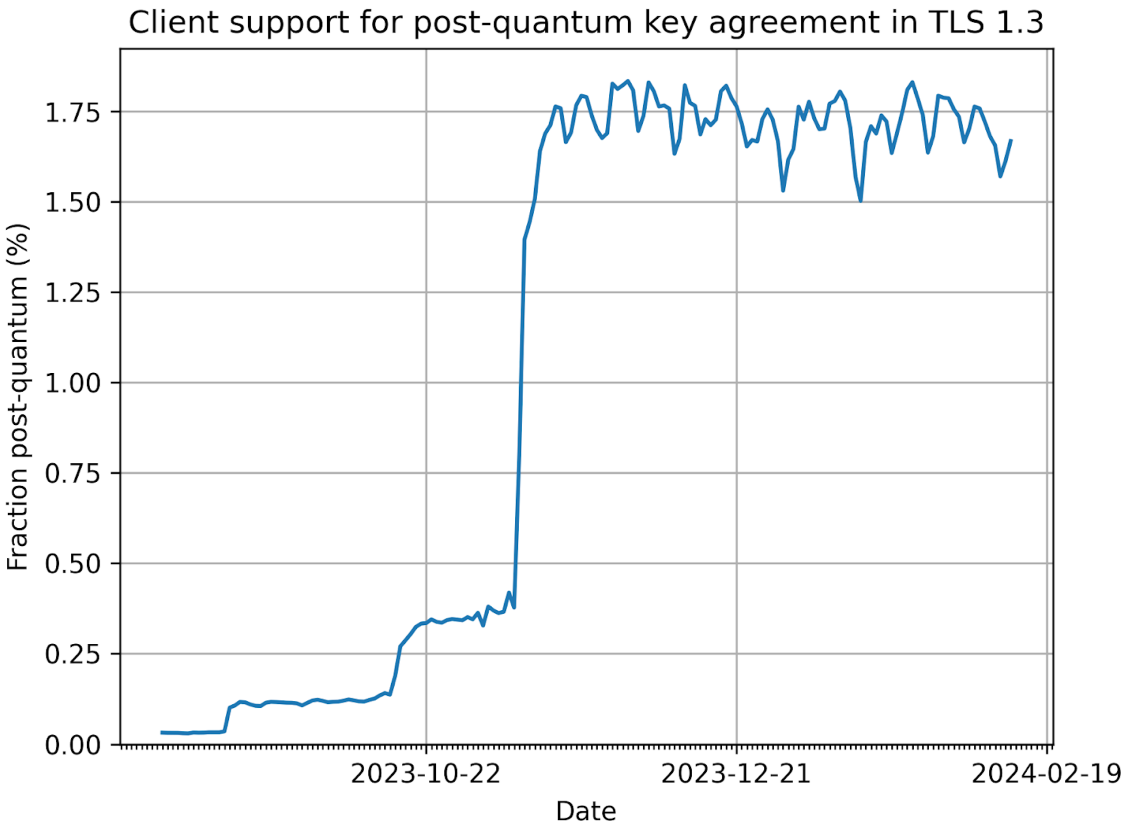
[ ] Updated applications

[ ] CBOMs to let you know which support what

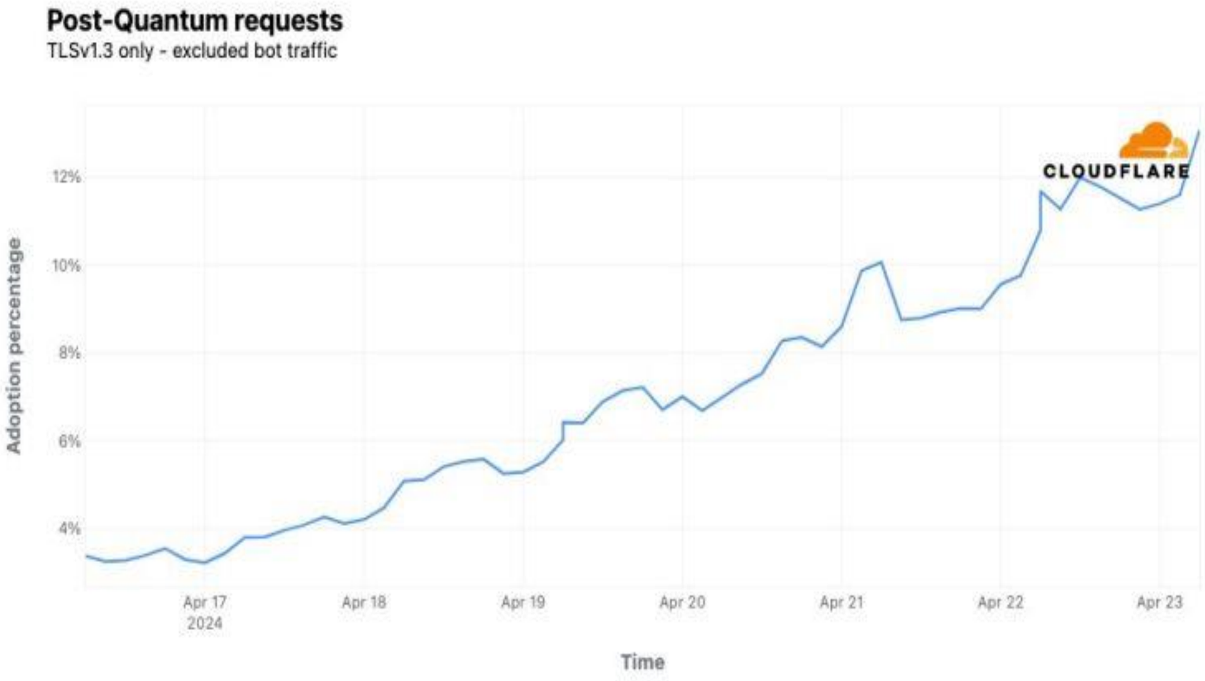
S/MIME protocol needs to be updated!

Key sizes and performance are different and sometimes worse, but not substantially so.

INDUSTRY HAS BEGUN MOVING TOWARDS PQC

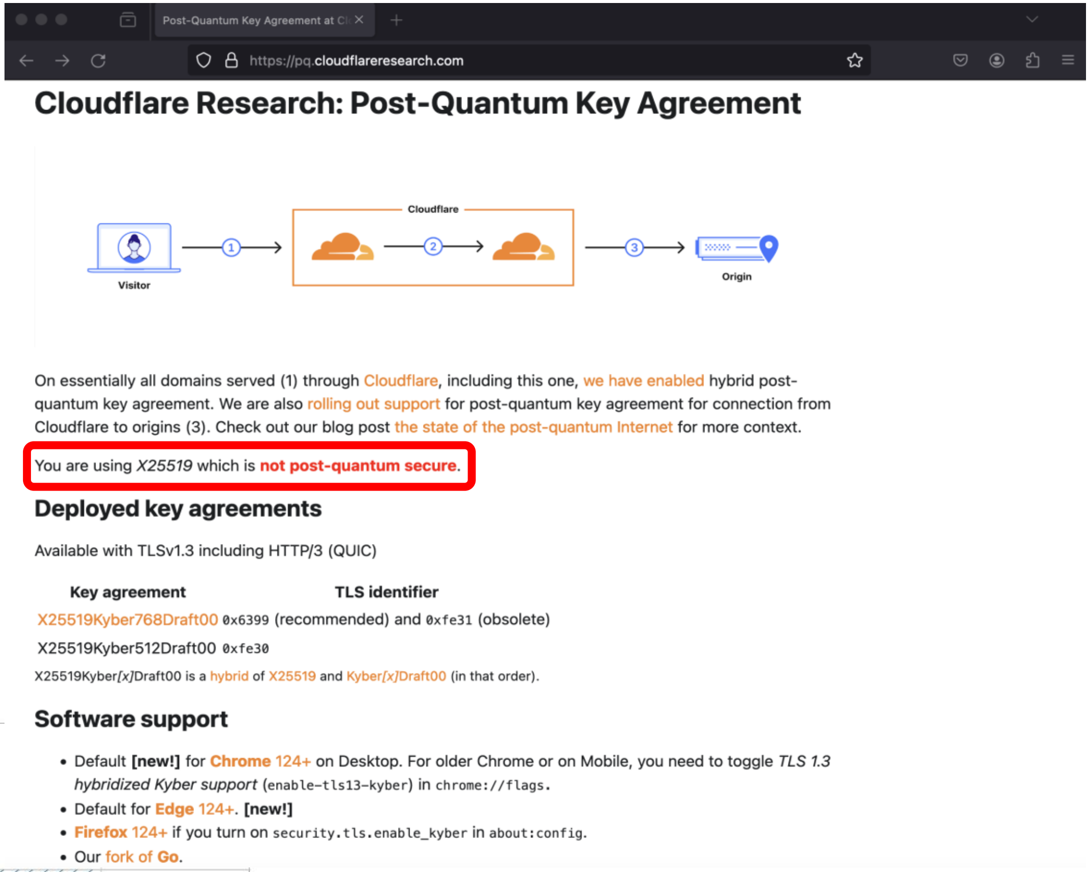


From **October 2023** to **February 2024** nearly **2% of all TLS 1.3** connections established with **Cloudflare** are secured with **PQC**



From **April 17th 2024** to **April 23rd 2024** nearly **13% of all TLS 1.3** connections established with **Cloudflare** are secured with **PQC**

ONE CLIENT AT A TIME (TLS FOR NOW, EMAIL SOON?)



Post-Quantum Key Agreement at Cl
https://pq.cloudflareresearch.com
Cloudflare
Visitor
Origin
1
2
3

Cloudflare Research: Post-Quantum Key Agreement

On essentially all domains served (1) through Cloudflare, including this one, we have enabled hybrid post-quantum key agreement. We are also rolling out support for post-quantum key agreement for connection from Cloudflare to origins (3). Check out our blog post the state of the post-quantum Internet for more context.

You are using *X25519* which is **not post-quantum secure**.

Deployed key agreements

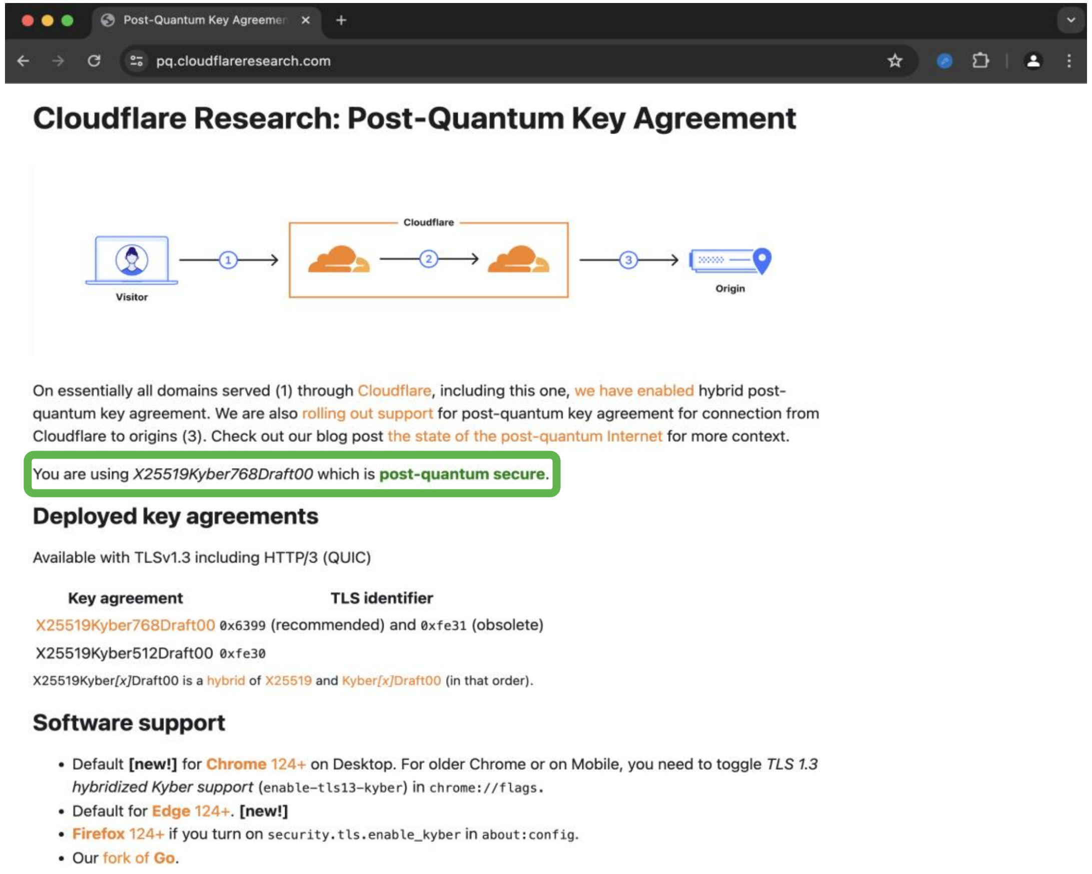
Available with TLSv1.3 including HTTP/3 (QUIC)

Key agreement	TLS identifier
X25519Kyber768Draft00	`0x6399` (recommended) and `0xfe31` (obsolete)
X25519Kyber512Draft00	`0xfe30`

X25519Kyber*[x]*Draft00 is a hybrid of X25519 and Kyber*[x]*Draft00 (in that order).

Software support

- Default **[new!]** for **Chrome** 124+ on Desktop. For older Chrome or on Mobile, you need to toggle *TLS 1.3 hybridized Kyber support* (`enable-tls13-kyber`) in `chrome://flags`.
- Default for **Edge** 124+. **[new!]**
- **Firefox** 124+ if you turn on `security.tls.enable_kyber` in `about:config`.
- Our fork of **Go**.



Cloudflare Research: Post-Quantum Key Agreement

On essentially all domains served (1) through Cloudflare, including this one, we have enabled hybrid post-quantum key agreement. We are also rolling out support for post-quantum key agreement for connection from Cloudflare to origins (3). Check out our blog post the state of the post-quantum Internet for more context.

You are using *X25519Kyber768Draft00* which is **post-quantum secure**.

Deployed key agreements

Available with TLSv1.3 including HTTP/3 (QUIC)

Key agreement	TLS identifier
X25519Kyber768Draft00	`0x6399` (recommended) and `0xfe31` (obsolete)
X25519Kyber512Draft00	`0xfe30`

X25519Kyber*[x]*Draft00 is a hybrid of X25519 and Kyber*[x]*Draft00 (in that order).

Software support

- Default **[new!]** for **Chrome** 124+ on Desktop. For older Chrome or on Mobile, you need to toggle *TLS 1.3 hybridized Kyber support* (`enable-tls13-kyber`) in `chrome://flags`.
- Default for **Edge** 124+. **[new!]**
- **Firefox** 124+ if you turn on `security.tls.enable_kyber` in `about:config`.
- Our fork of **Go**.

THE CHALLENGE

With increased connectivity, the scale of what needs to be updated also increases.

Maintain
Interoperability

Migrate Critical
Systems Faster

Reduce
Switching Costs

QUANTUM-SAFE CRYPTO IN S/MIME

Quantum-safe algorithms are not a drop-in replacement for RSA / ECC

With RSA and ECC, you can use the same key for both signing and asymmetric encryption.
With quantum-safe cryptography, those operations use two separate algorithms.

Two cert email encryption/signing solutions are pretty easy to upgrade, just replace the key encryption and content signing algorithms.

One cert signing will need more significant changes (and might not be possible or prudent).

There are probably other things I’ve forgotten.

QUANTUM RESISTANCE IN THE REAL WORLD

ML-KEM	ML-DSA	SLH-DSA	FN-DSA
Crystals-Kyber	Crystals-Dilithium	SPHINCS+	FALCON
FIPS-203	FIPS-204	FIPS-205	Proposed Name-Released
Key encapsulation for recipient keys	Signatures for authentication	If you like hash-based signatures instead	Maybe someone will find a use for this, some day

FINISHING THE JOB

1. Needs to be coordinated across all S/MIME capable systems. Which is why we need standards!
2. Most important: must be able to use a KEM to transport the content encryption key to each recipient.

   https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-kemri/

   CMS is the message format that S/MIME is built on top of

   KEM = key encapsulation mechanism

   RI = recipient info

KEMRI

Field (type)	Value
CMSVersion	0
RecipientIdentifier	issuerAndSerialNumber or subjectKeyIdentifier (a hash)
KEMAlgorithmIdentifier	Probably Crystals-Kyber / ML-KEM (shared secret -> kek)
OCTET STRING	KEM ciphertext (the important part)
KeyDeriviationAlgorithmIdentifier	How the key was produced
INTEGER	Size of key encrypting key
UserKeyingMaterial (optional)	Additional context information as input for key derivation
KeyEncryptionAlgorithmIdentifier	How the key was encrypted
EncryptedKey (OCTET STRING)	Content encryption and authentication key encrypted with the key encrypting key

STATUS AND NEXT STEPS

04

QUANTUM-SAFE S/MIME STANDARDS

- Need algorithms for KEMs and Signing: NIST, hopefully this summer.
- Need EE certs:
  - Kyber certificates: https://datatracker.ietf.org/doc/draft-ietf-lamps-kyber-certificates/
  - Dilithium certificates: https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/
  - Other, more complicated types exist; these are the “basic” ones.
- Need roots and chains
  - more or less what you expect, and needed for other things too
  - Just need a quantum-safe signature algorithm (If you can sign a wrench, you can sign a certificate)
- Need updated recipient info: https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-kemri/
- Need updated S/MIME standard: LAMPS working group, not started.

LONG-TERM SIGNATURES

Signatures being generated today are vulnerable to forgery in the future.

A successful attack with a quantum computer recovers the private key from the public key, so the contents can be altered and re-signed. Timestamps can also be forged.

Solution:

Attest to the classic signature with a quantum-safe signature

There's a brief window of time before quantum computers arrive when such an attestation can breathe new life into a digital signature that would otherwise lose its trust soon.

digicert®

Tim.Hollebeek@digicert.com

EXTENDING TRUST

MANAGING TRUST

ESTABLISHING TRUST

COMPLIANCE

AUTHORING STANDARDS

DIGITAL TRUST