moz://a

Post Quantum Crypto and Mozilla

Crypto beyond TLS

8.11.2019

Dr. Franziskus Kiefer

SURF Summit, Vienna 2019

Agenda

Crypto @ Mozilla

PQ Crypto @ Mozilla

Crypto @ Mozilla

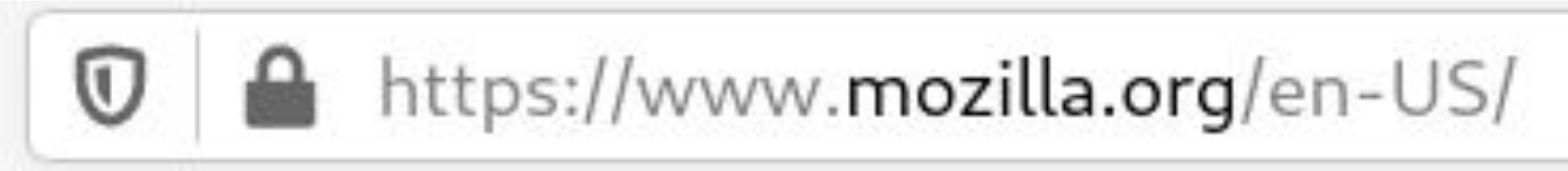
There’s more than TLS

Motivation

- PQC Algorithms have significantly different properties
- Selection of “right” algorithms heavily depends on use-case
- Showcase different use cases

Main Question

How can we select the right algorithm for each use case?



https://www.mozilla.org/en-US/

Crypto in TLS

Authentication

- RSA-PKCS1
  - SHA-256, SHA-384, SHA512
  - SHA-1
- RSA-PSS
  - SHA-256, SHA-384, SHA512
- ECDSA
  - P-256, P-384, P-521
  - SHA-1
- EdDSA
  - x25519, x448
- Custom

Transport Encryption

- AES-GCM
  - 128, 256
- AES-CCM 128
- AES-CCM-8 128
- ChaCha20Poly1305

Key Exchange

- P-256, P-384, P-521
- x25519, x448
- FFDHE-2048, FFDHE-3072, FFDHE-4096, FFDHE-6144, FFDHE-8192
- Custom DHE or ECDHE

TLS is a very specific use-case

for Mozilla

- Secure transport of content over the internet
- High number of handshakes
    - how many?
- Protocol optimisations to avoid full handshake
- Standardised protocol that’s hard to change

Updates and Integrity

- Firefox Updates
- Firefox extensions
- Involves PKI and HSMs

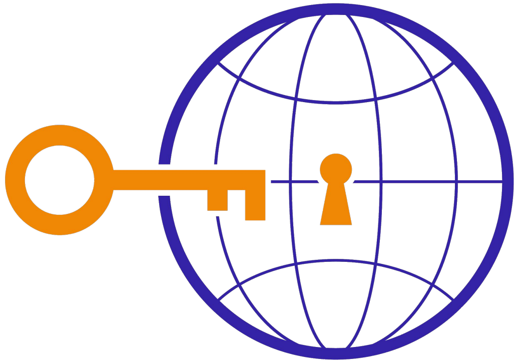
Device Linking & Discovery

Link browser instances

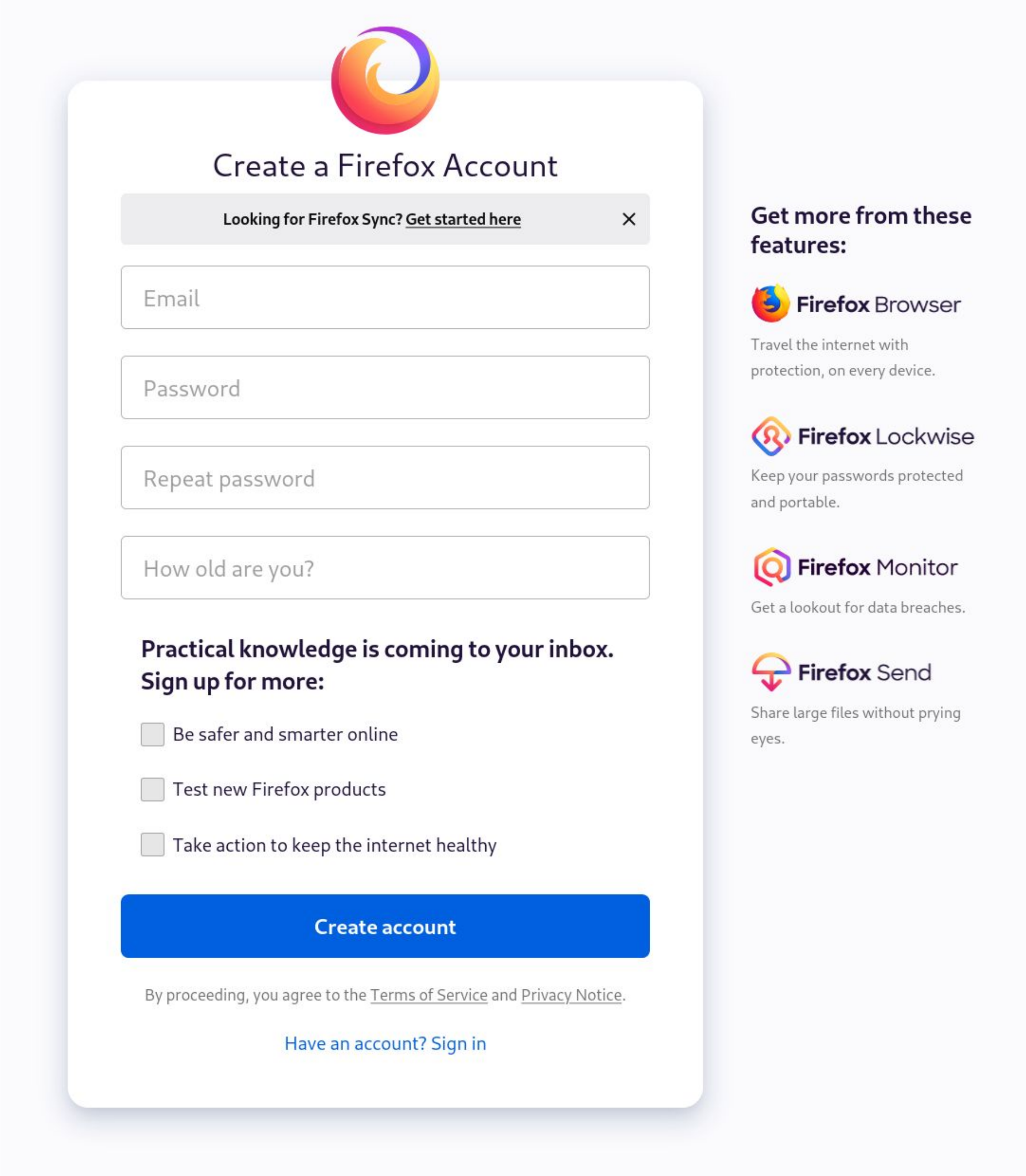
- debugging
- simplified login on mobile/TV

Web Authentication

- An API for accessing Public Key Credentials
- Can use hardware tokens
  - hard to replace
  - resource constraint



Firefox Accounts & Sync



Create a Firefox Account

Looking for Firefox Sync? Get started here ✕

Email

Password

Repeat password

How old are you?

Practical knowledge is coming to your inbox. Sign up for more:

□ Be safer and smarter online

□ Test new Firefox products

□ Take action to keep the internet healthy

Create account

By proceeding, you agree to the Terms of Service and Privacy Notice.

Have an account? Sign in

Get more from these features:

Firefox Browser

Travel the internet with protection, on every device.

Firefox Lockwise

Keep your passwords protected and portable.

Firefox Monitor

Get a lookout for data breaches.

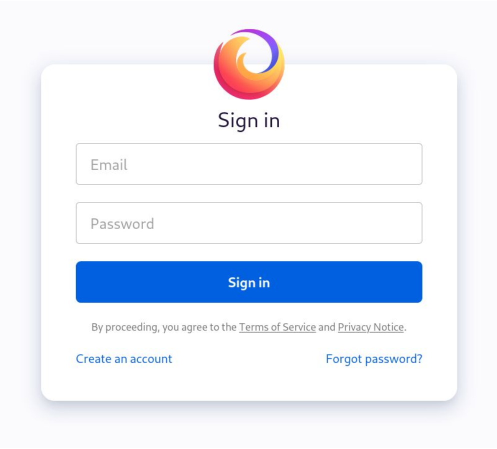
Firefox Send

Share large files without prying eyes.

Firefox Accounts & Sync

Sync Browser Data

- Logins and Passwords
- Addresses
- Bookmarks
- Open Tabs
- History

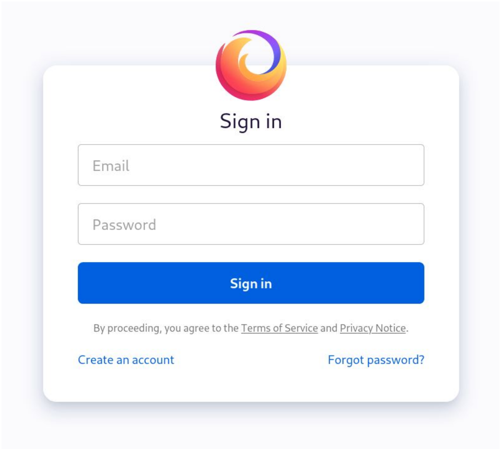


By proceeding, you agree to the Terms of Service and Privacy Notice.

Firefox Accounts & Sync

Firefox Account

- SSO provider
- Access to services



Sign in

Email

Password

Sign in

By proceeding, you agree to the Terms of Service and Privacy Notice.

Create an account

Forgot password?

Telemetry Data

- Firefox telemetry doesn’t use PETs (yet)
- PRIO
  - allows privacy-preserving origin telemetry (somewhat)

DevSecOps

- Securing development & operations
- AWS, GCP, Azure, …
- SOPS
  - Secrets OPerationS

Crypto Code @ Mozilla

The Crypto Library

NSS

- Mozilla has (some) control over NSS
- Used for most things in the browser
    - not all though

Other Crypto Code

- Server-side implementations
  - Mostly use Go crypto
  - Some JavaScript crypto
- Rust 3rd party libraries in Firefox
- Openssl
  - used all over the place for services

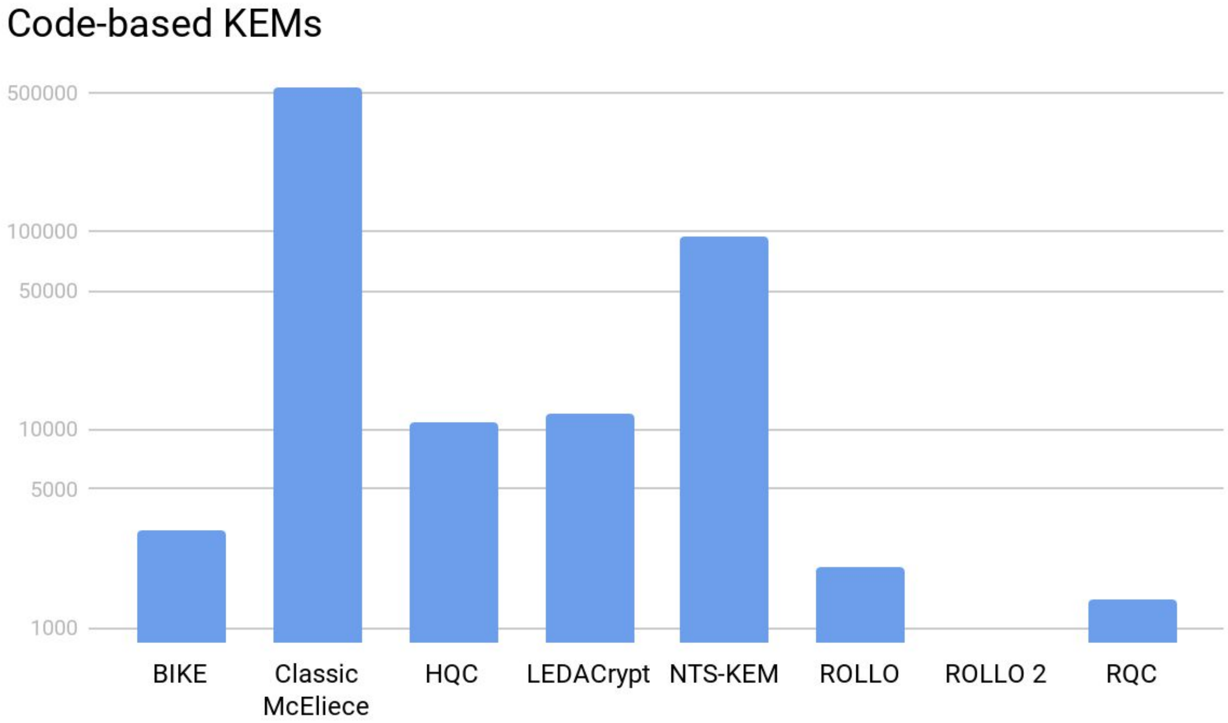
Assessing NIST candidates

for Mozilla

- Key size
- Key generation performance
- KEM message size
- KEM performance
- Sign/Verify performance
- Signature size

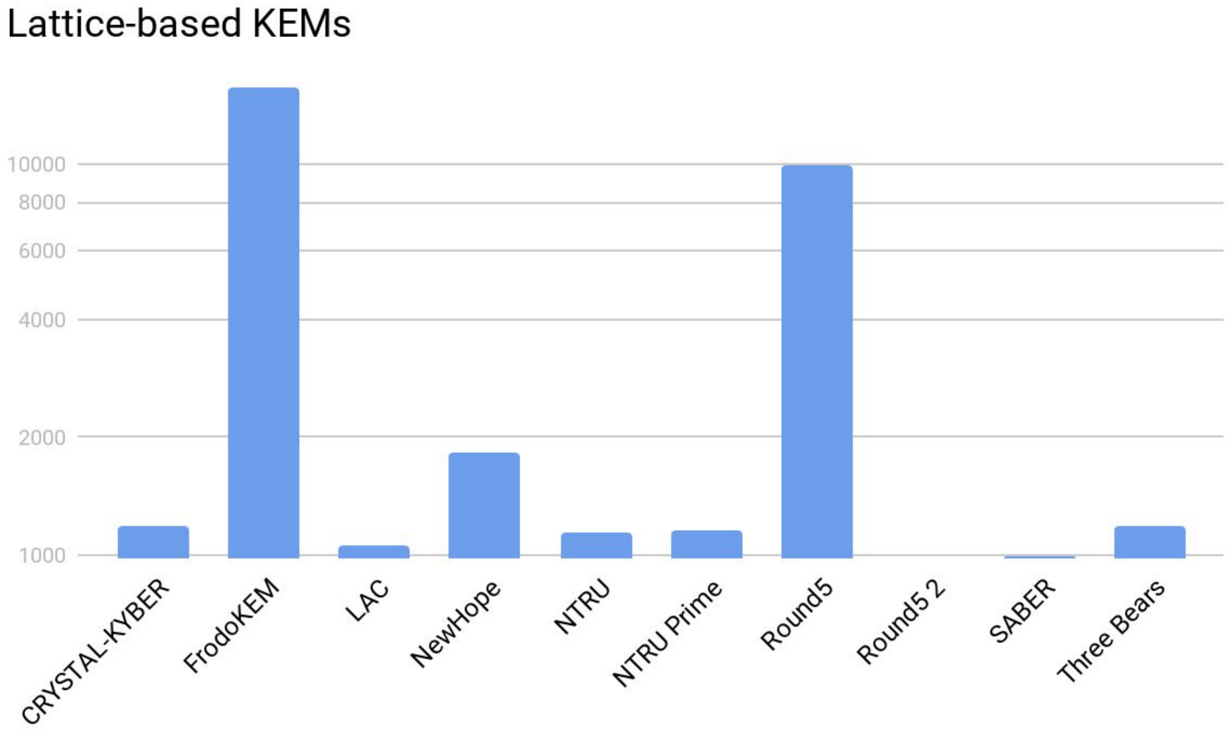
NIST candidates

Level 3 Public Key Size



NIST candidates

Level 3 Public Key Size



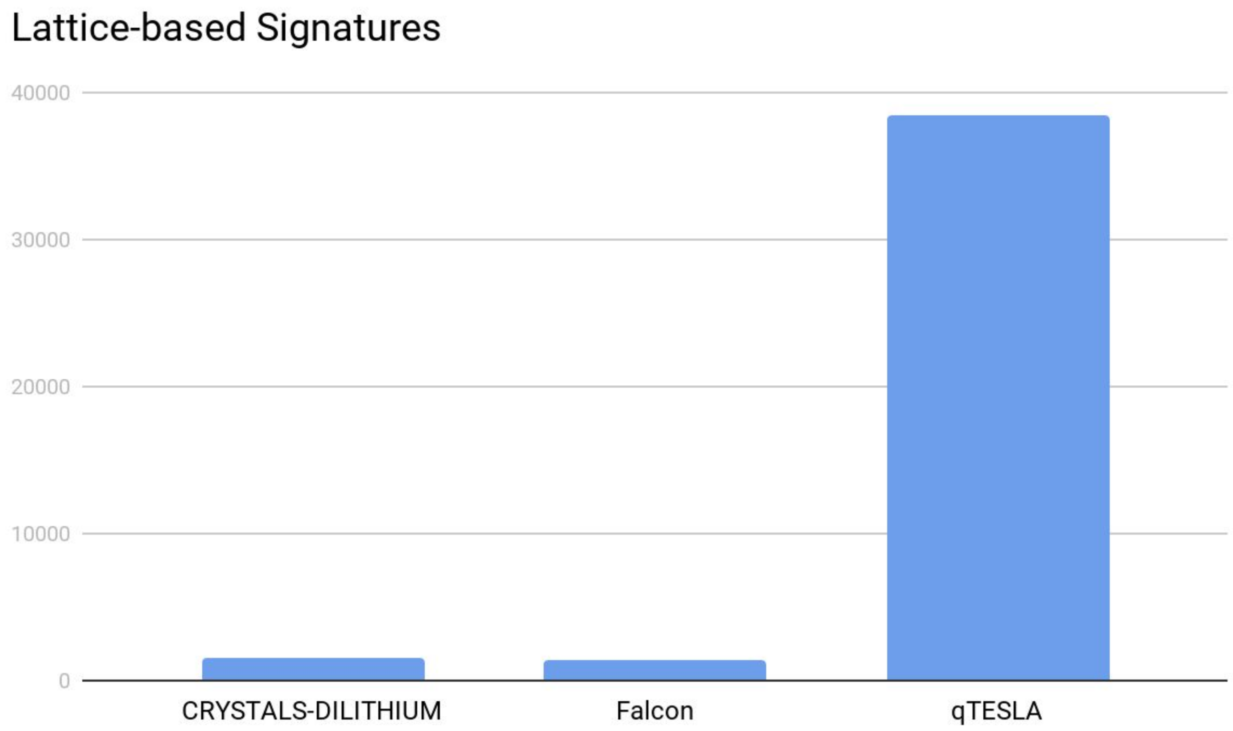
NIST Candidates

Other KEMs

- SIKE
  - 462 or 273 bytes Public keys

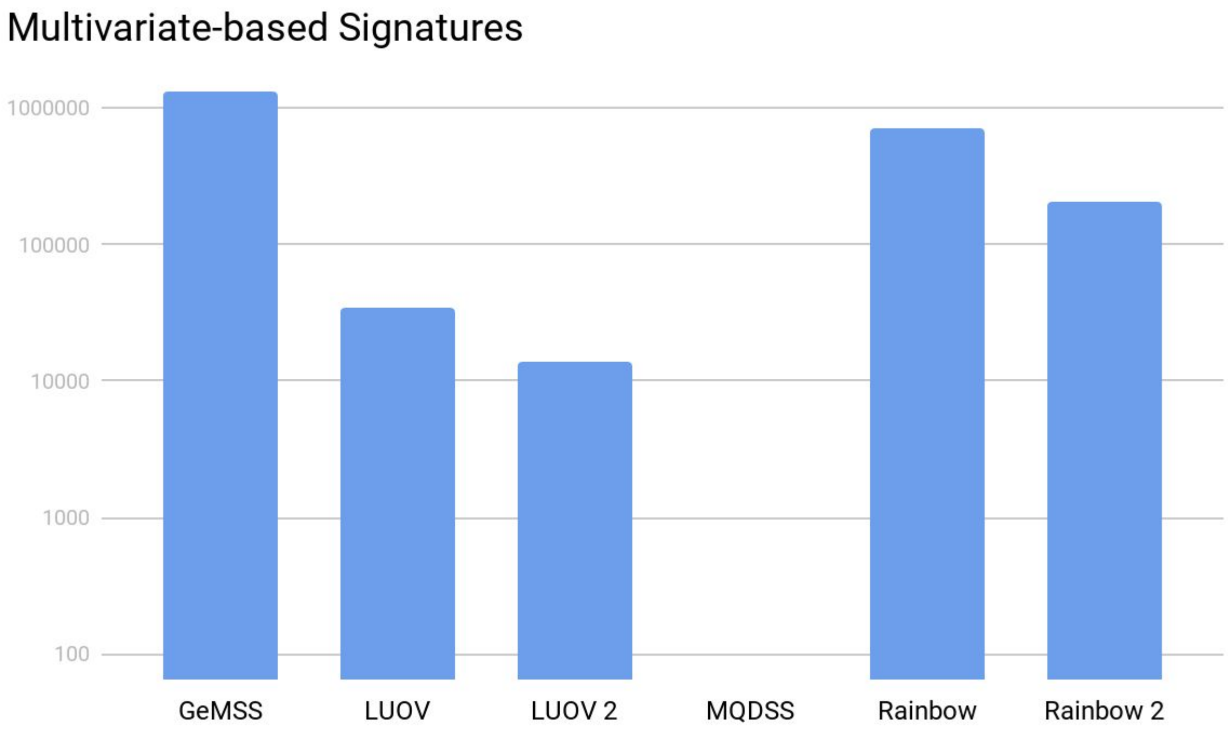
NIST Candidates

Level 3 Public Key Size



NIST Candidates

Multivariate Signatures



NIST Candidates

Hash-based Signatures

- SPHINCS+
  - 48
- Picnic
  - 48

Assess Candidates

Run experiments

Get code ready

moz://a

Thank You