CryptPad

Experiments on Post-Quantum Cryptography

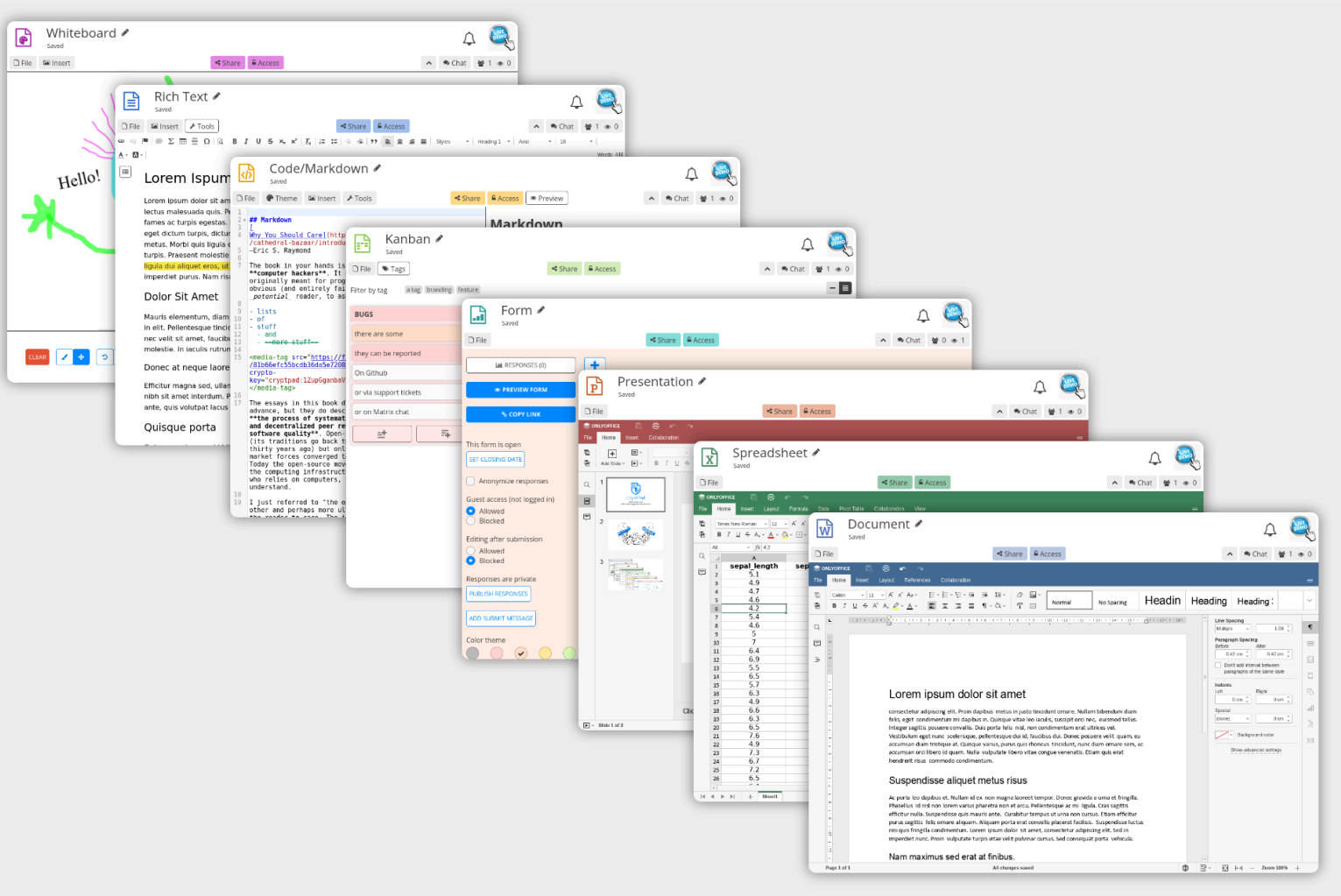
Fabrice Mouhartem, Iulian-Tudor Scutaru

July 1st 2026

@Pass the Salt 2026

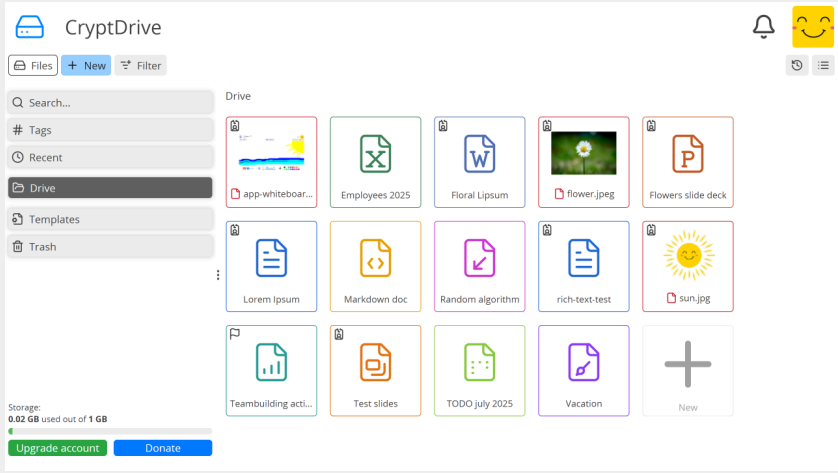
Introduction

CryptPad


Whiteboard
Rich Text
Code/Markdown
Kanban
Form
Presentation
Spreadsheet
Document
Lorem ipsum dolor sit amet
Suspendisse aliquet metus risus
Nam maximus sed erat at finibus.

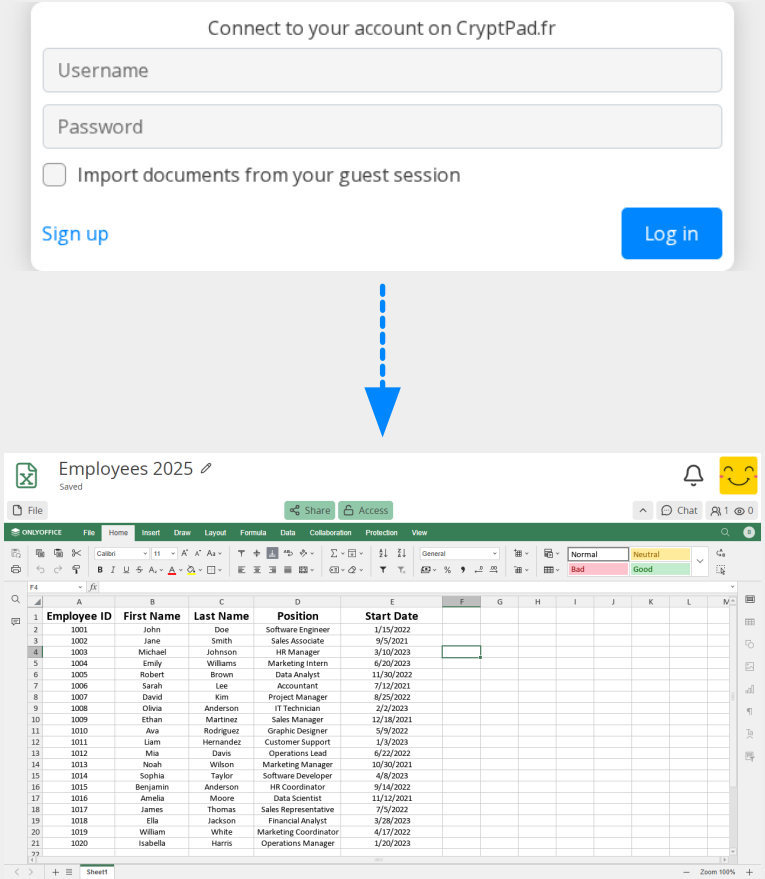
CryptPad

- Office suite
  - Several built-in document types (forms, office, diagrams, …) + collaboration tools (teams, calendars, …)
- Real-time collaboration
- End-to-end encrypted
- For everyone:
  - “Everything in one place” web app
  - Accessibility
  - Familiar interface



Secure collaboration: put the Crypt in CryptPad

- Secure login: key derivation
- Documents are encrypted with their own encryption key (view right)
- Documents can be edited with their individual signature (edit right)
- More complex derivations for forms

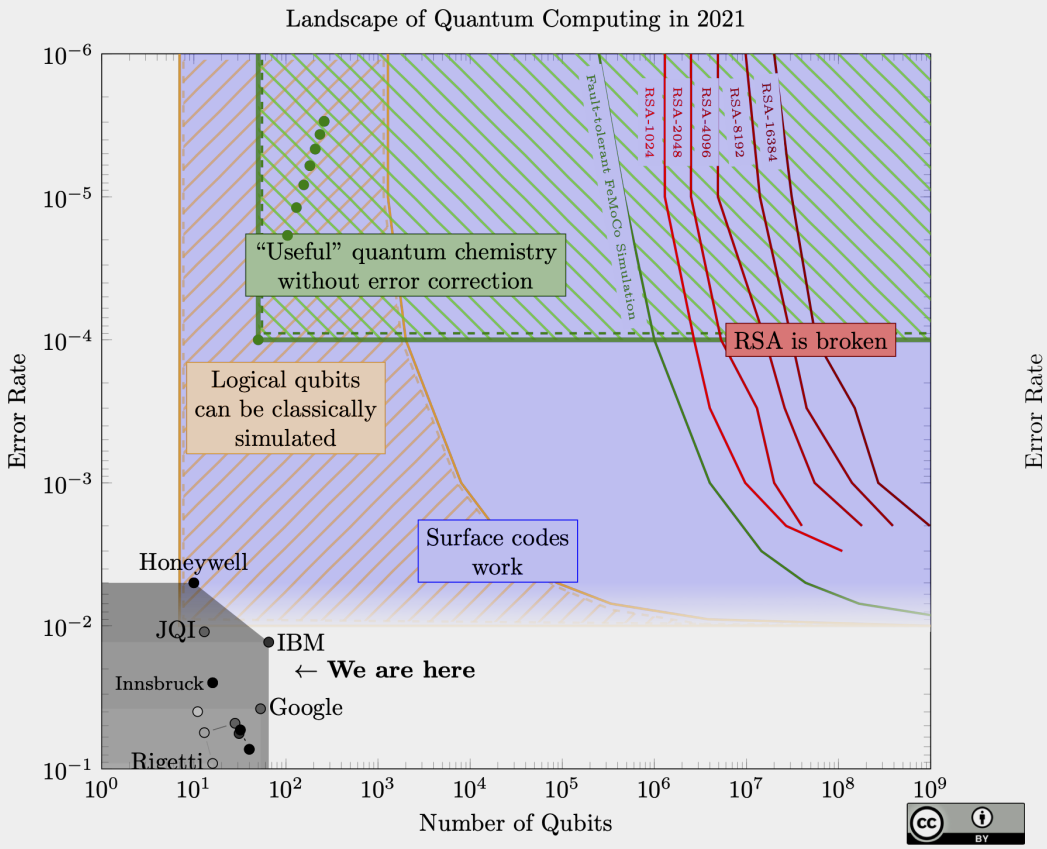


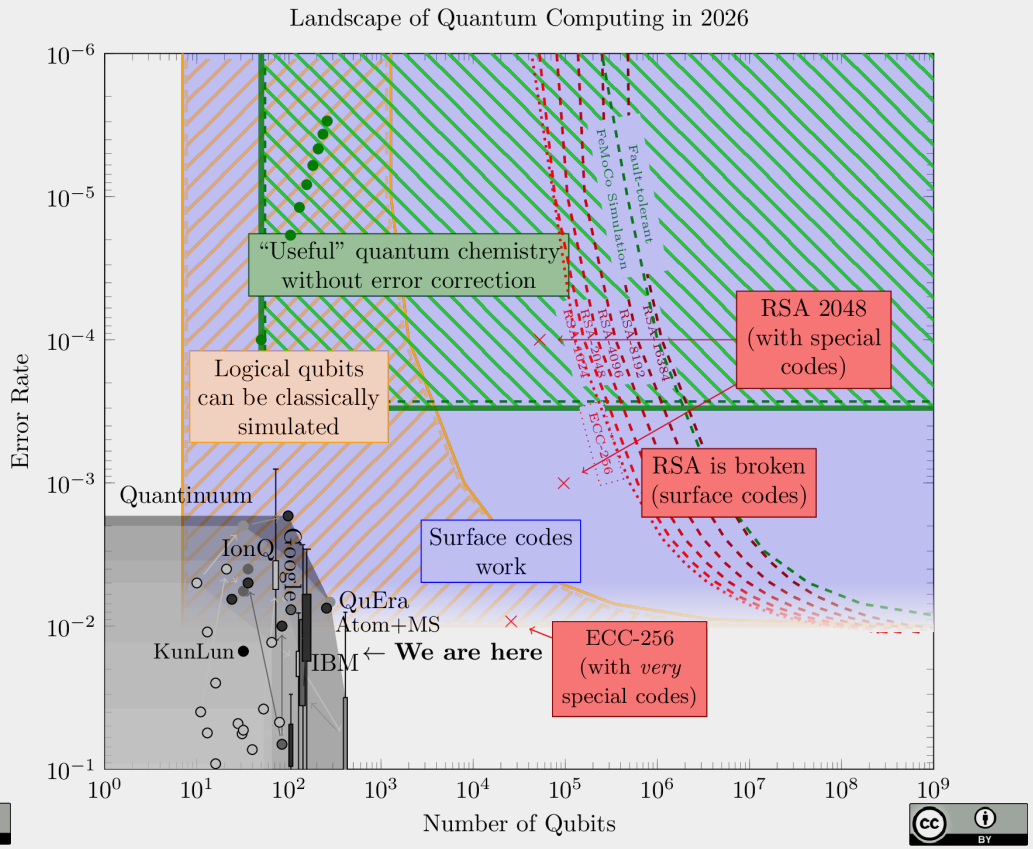
Secure collaboration: put the Crypt in CryptPad

- Mailbox system for inter-user communications: PKE
- Interuser chat: PKE
- Badges: signatures
- Other stuff under the hood: hash functions, PRNG, ...

More details in our white paper:
> https://blueprints.cryptpad.org/document/whitepaper/

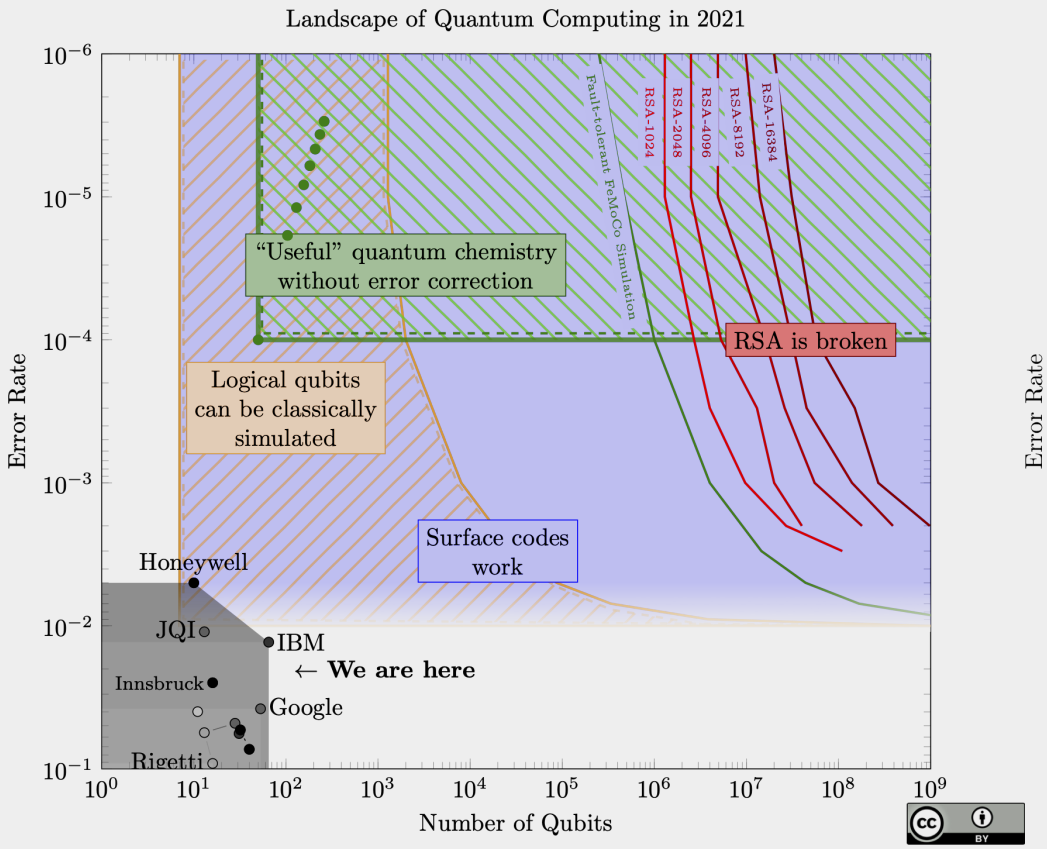
Quantum Threat

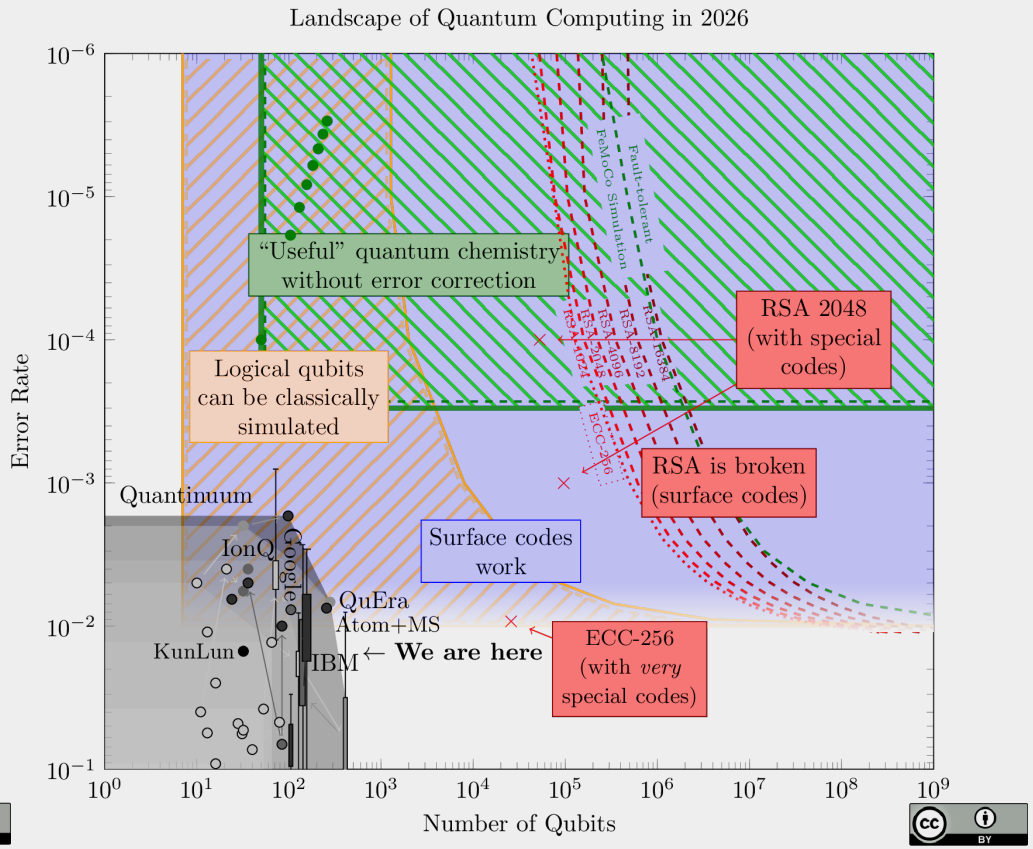




> https://sam-jaques.appspot.com/quantum_landscape

Quantum Threat

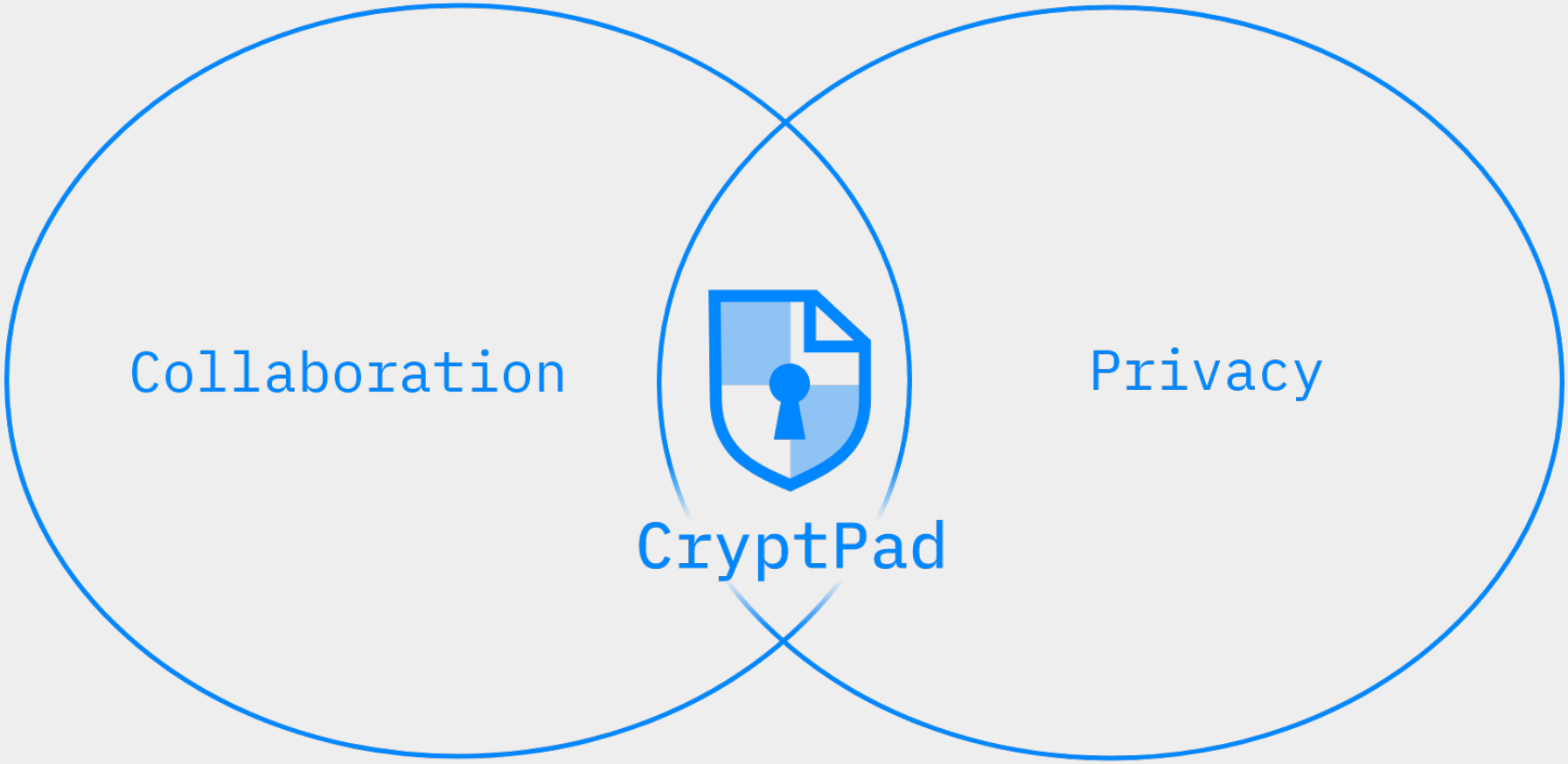




> https://sam-jaques.appspot.com/quantum_landscape

- Agencies recommendation: ASAP

You can have Both



Yes, you can have both

Post-Quantum CryptPad

Our constraints

- Centralised service: server serves the client code
- Javascript (Node.js + browser compatibility)

Our constraints

- Centralised service: server serves the client code
- Javascript (Node.js + browser compatibility)
- (Authenticated) Symmetric Encryption: `xsalsa20-poly1305` (NIST Cat 5)
- Hash function: `SHA-512` (NIST Cat 5)
- To be replaced:
  - Encryption + Signature: ECC with `Curve25519`

Our constraints

- Centralised service: server serves the client code
- Javascript (Node.js + browser compatibility)
- (Authenticated) Symmetric Encryption: `xsalsa20-poly1305` (NIST Cat 5)
- Hash function: `SHA-512` (NIST Cat 5)
- To be replaced:
  - Encryption + Signature: ECC with `Curve25519`
- No crypto-agility 🙃

Our constraints

- Centralised service: server serves the client code
- Javascript (Node.js + browser compatibility)
- (Authenticated) Symmetric Encryption: `xsalsa20-poly1305` (NIST Cat 5)
- Hash function: `SHA-512` (NIST Cat 5)
- To be replaced:
  - Encryption + Signature: ECC with `Curve25519`
- No crypto-agility 🙃
- E2EE: client-side migration
  - Already in place 🎉

JS crypto library

- Few candidates (in 2025):
  - **Noble**
  - **Crystal-Kyber-js**
  - **scintilla-network**
  - **HPKE-js**
- Noble was selected
  - General purpose crypto library with several implemented PQC standards
  - Up to date
  - WASM & good performances
  - **Node.js** compatible

Crypto-Agility

The ability to switch between different cryptography algorithms

- CryptPad was not built for that for historical reasons (technical debt)

Crypto-Agility

The ability to switch between different cryptography algorithms

- CryptPad was not built for that for historical reasons (technical debt)
- Would make PQC experiments easier

Crypto-Agility

The ability to switch between different cryptography algorithms

- CryptPad was not built for that for historical reasons (technical debt)
- Would make PQC experiments easier
- Was thus implemented in the product 🎉

Algorithm Selection

Caveats

Made in 2025:

- No FIPS for **FN-DSA** (Falcon)
- **HQC** was not selected yet

Algorithm Selection

Caveats

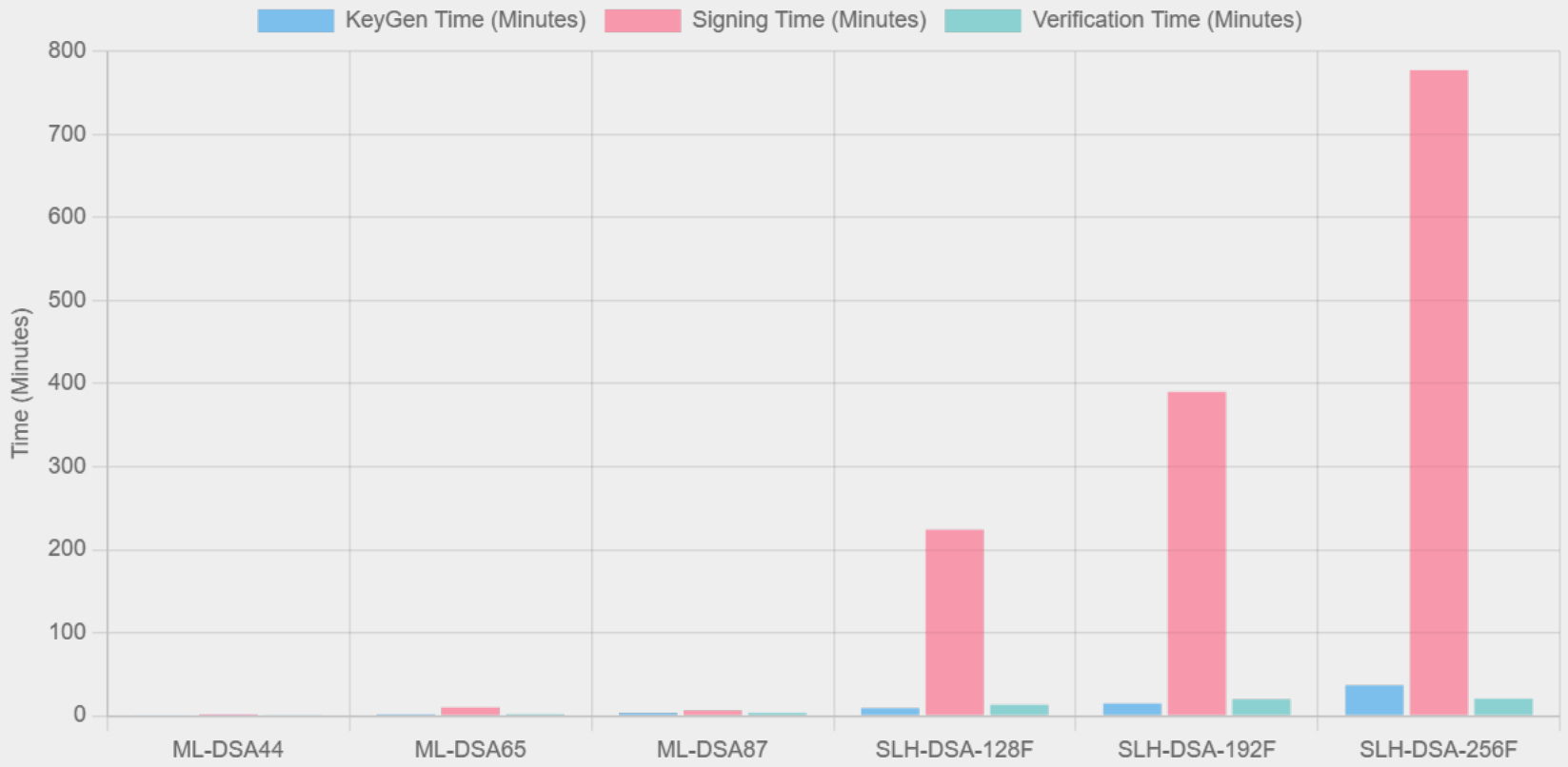
Made in 2025:

- No FIPS for **FN-DSA** (Falcon)
- **HQC** was not selected yet

- Signatures:
  - **ML-DSA** (Dilithium)
  - **SLH-DSA** (Sphincs+)
- Encryption
  - **ML-KEM** (Kyber)

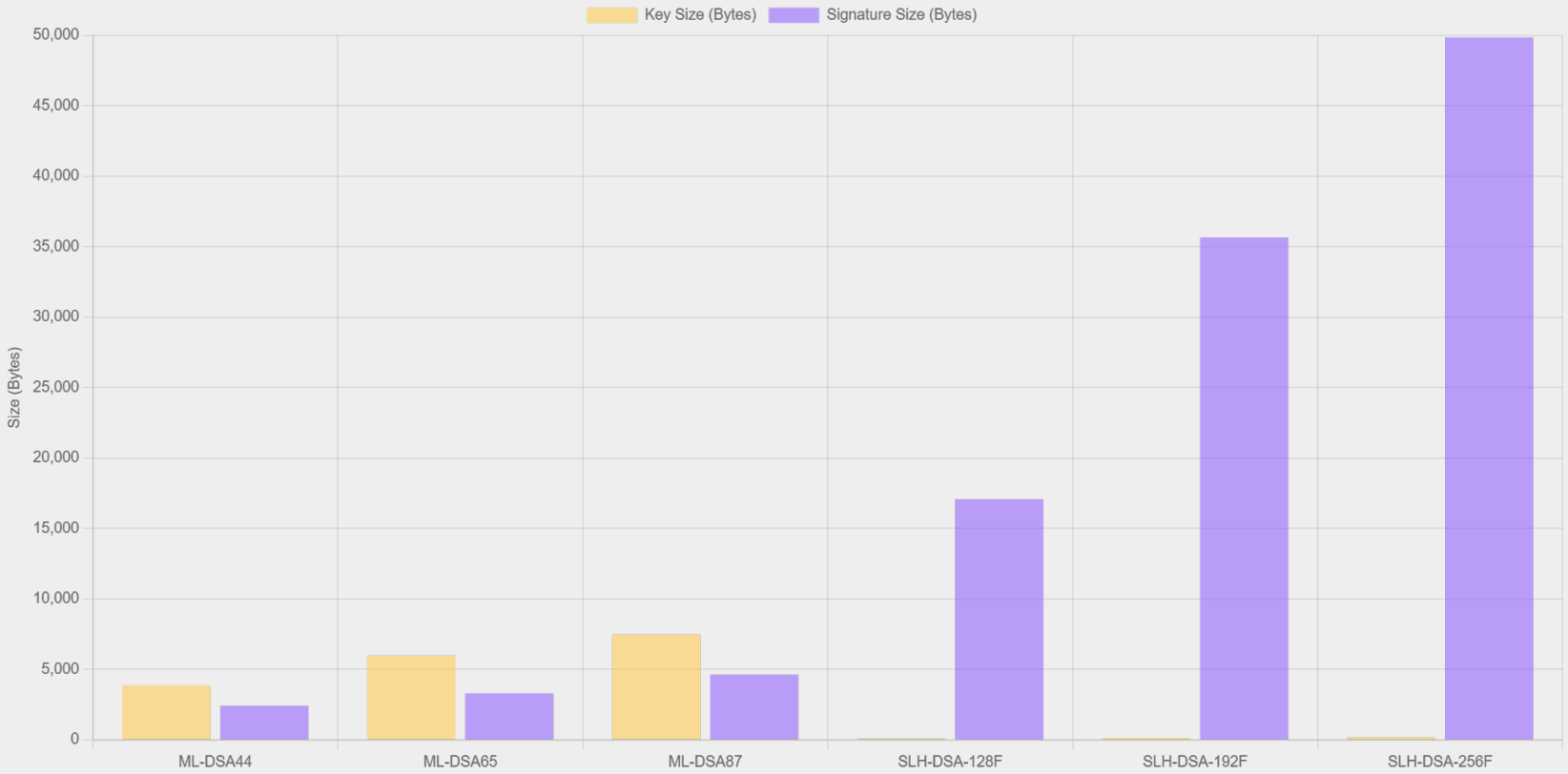
Algorithm Selection

30k Signatures Time (firefox)



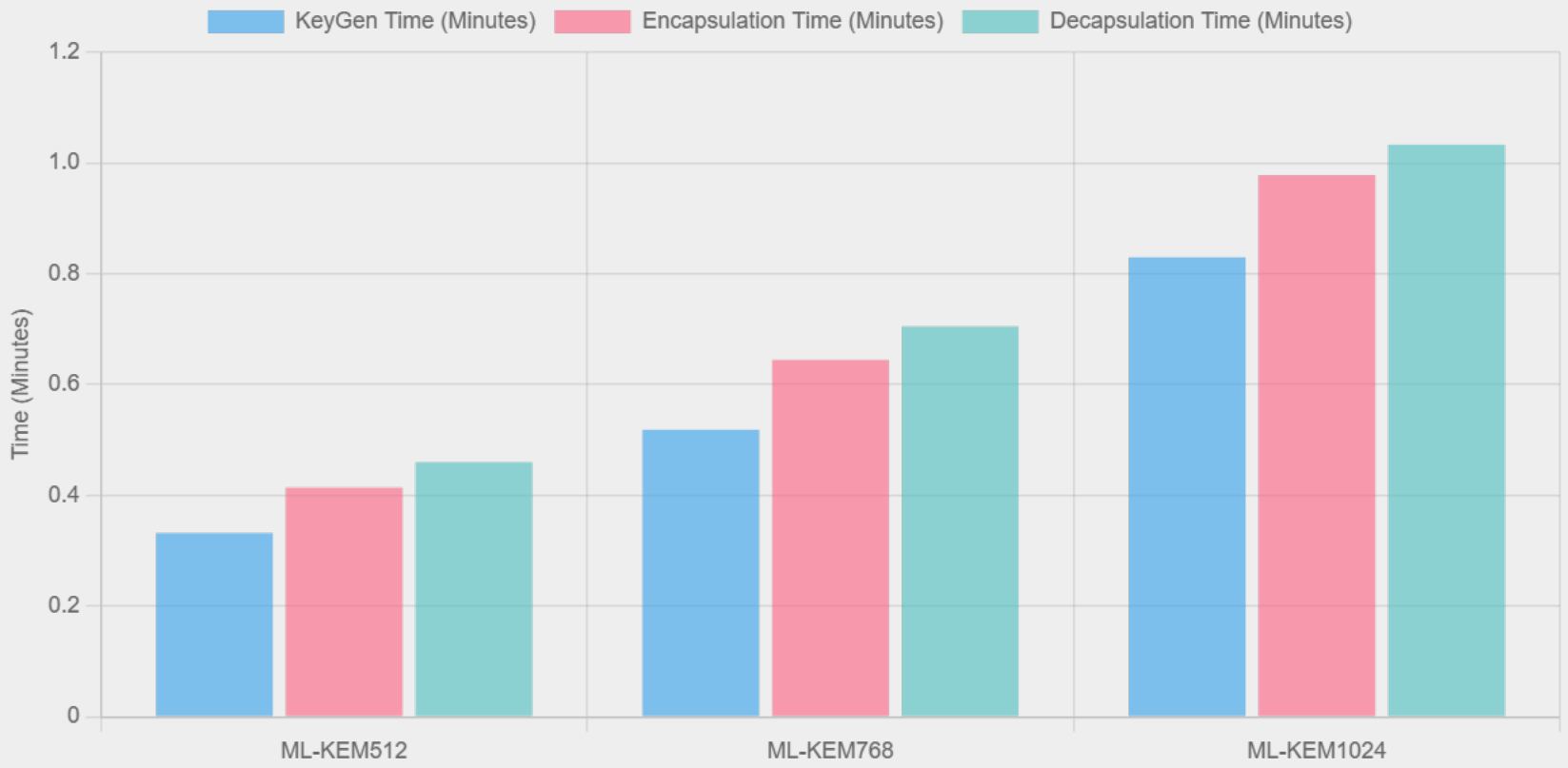
Algorithm Selection

30k Signatures Storage



Algorithm Selection

30k KEM (firefox)



CryptPad Simulator

Goal: simulate the cryptography average use on CryptPad.fr

- https://github.com/cryptpad/pqc-mockup
- Simulate exchanges based on our metrics for average use
  - Accounts creation
  - Document opening/creation
  - Sending modifications
  - Sharing files internally

CryptPad Simulator 2025

- Individual operations (average)

Operation Time (ms)	Encrypt	Decrypt	Sign	Verify
Classical	3.77	8.53	1.61	3.66
Post-Quantum	21.66	8.58	9.28	3.68

CryptPad Simulator 2025

- Individual operations (average)

Operation Time (ms)	Encrypt	Decrypt	Sign	Verify
Classical	3.77	8.53	1.61	3.66
Post-Quantum	21.66	8.58	9.28	3.68

- Overall (1 document with 60k edits)

Metric	Time(s)	
Classical	935.817	
Post-Quantum	33,436.689	35.7× slower

CryptPad Simulator 2025

- Individual operations (average)

Operation Time (ms)	Encrypt	Decrypt	Sign	Verify
Classical	3.77	8.53	1.61	3.66
Post-Quantum	21.66	8.58	9.28	3.68

- Overall (1 document with 60k edits)

Metric	Time(s)	
Classical	935.817	
Post-Quantum	33,436.689	35.7× slower

> Quite the impact on the user experience...

Bottlenecks

1. Encryption operations (2.8× slower)
2. Signing operations (2.8× slower)
3. Key storage requirements (up to 81× larger)

Bottlenecks

1. Encryption operations (2.8× slower)
2. Signing operations (2.8× slower)
3. Key storage requirements (up to 81× larger)

> What is the impact on actual user experience?

Implementation in CryptPad

> https://github.com/cryptpad/cryptpad/tree/crypto-agility

- Everything is done in a hybdrid (PQC + Classical) manner
- Real world document edition works well
- Loading a drive is acceptable

Implementation in CryptPad

> https://github.com/cryptpad/cryptpad/tree/crypto-agility

- Everything is done in a hybdrid (PQC + Classical) manner
- Real world document edition works well
- Loading a drive is acceptable
- Issues with non-interactive key exchange (NIKE) trick
- Our team system have significant overhead
  - More than 1 minute loading time with 5 drives on first use
  - (since then: background loading but not a full solution)
- No test under load

What next?

- Fine grain tuning on cryptography use
  - Need huge code refactor
  - Retrocompatibility
- UX changes?
  - The NIKE issue comes from internal chats with low usage
- ANSSI certifications

Conclusion

Conclusion

- PQC is important to guarantee security in the long run
- For CryptPad it's less urgent than for some other pieces of software
  - However some pressure is put: ANSSI will stop providing certifications for non quantum-resilient products in 2027
- Experiments showed that CryptPad collaboration engine needs refactoring before being quantum-resilient
- We are pursuing efforts in this direction

CryptPad

David	—	CryptPad Team Lead
Andreea	—	Developer
Daria	—	Developer
Diana	—	Developer
Fabrice	—	R&D Engineer
Wolfgang	—	R&D Engineer
Yann	—	Privacy Engineer
Zuzanna	—	Software Dev Engineer
Ludovic	—	XWiki CEO

Thank you for your attention

🎙️ Question time

- Stay in touch:
  - Blog: https://blog.cryptpad.org/
  - Mastodon: https://social.xwiki.com/@CryptPad/
  - Community forum: https://forum.cryptpad.org/