



CryptPad

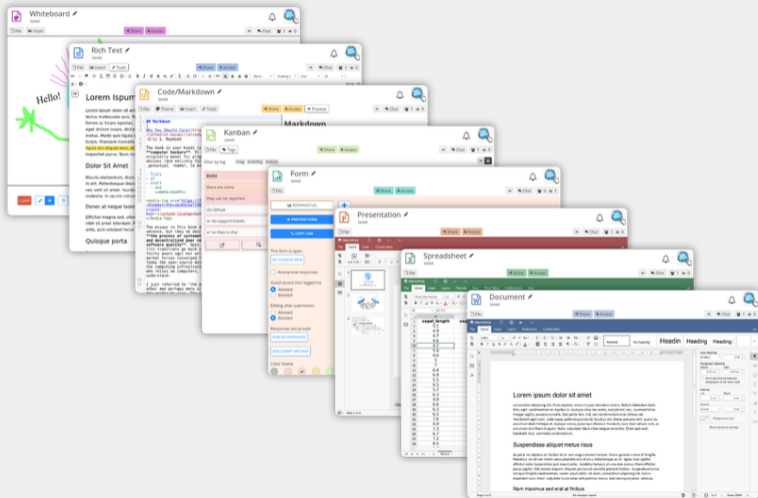
Securely collaborate with CryptPad

Fabrice Mouhartem

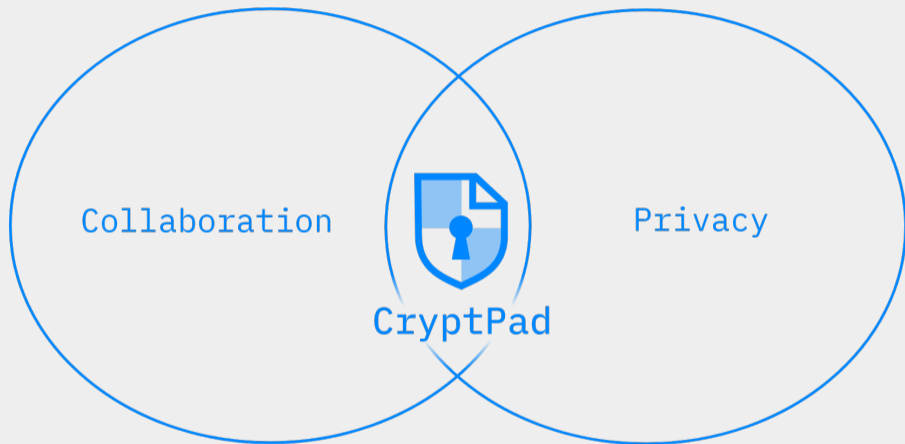
February 03, 2024

FOSDEM

CryptPad



Privacy-Friendly Collaborative Edition



Yes, you can have both

The
Intercept_

NAOMI
_KLEIN



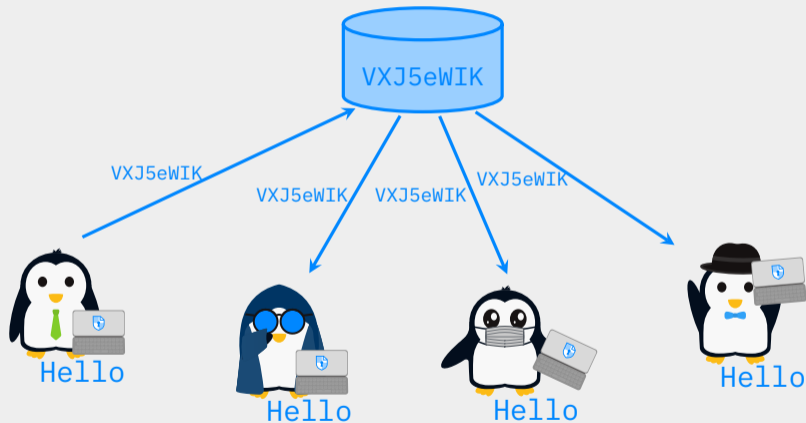
India Targets Climate Activists With the Help of Big Tech

Tech giants like Google and Facebook appear to be aiding and abetting a vicious government campaign against Indian climate activists.

Naomi Klein

February 27 2021, 9:00 a.m.

End-to-End Encrypted Collaborative Edition





- ▶ Cryptographic analysis & prepare for the future



- ▶ Cryptographic analysis & prepare for the future
- ▶ Possible improvements:
 - Cryptographic agility
 - Password Recovery
 - Revocation

An example: Password Recovery

Cryptography-Driven Design

- ▶ Users are identified with a signature public key
- ▶ The relation between the public key and the password is one-way

An example: Password Recovery

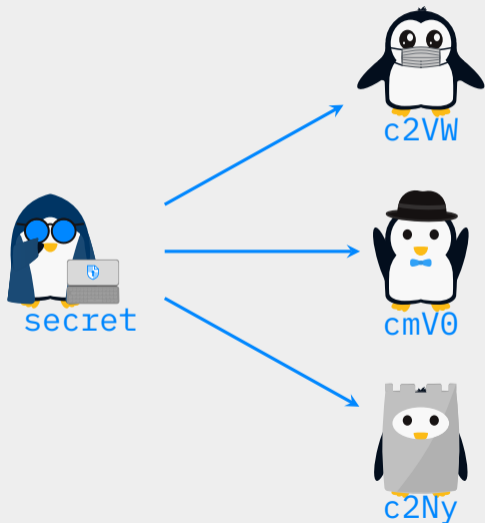
Cryptography-Driven Design

- ▶ Users are identified with a signature public key
- ▶ The relation between the public key and the password is one-way

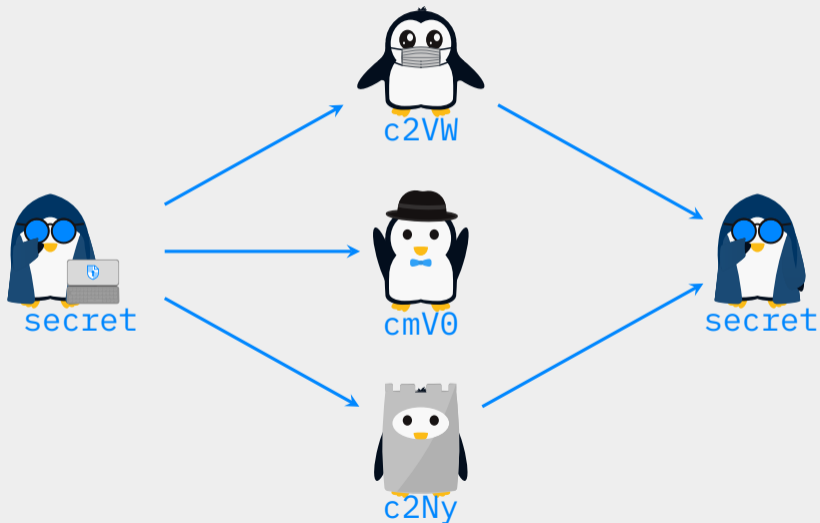
How to Solve this Problem?

- ▶ With more cryptography:
 - Linear secret sharing [RS60, Sha79]

Social Secret Sharing: in Theory



Social Secret Sharing: in Theory



Social Secret Sharing: in Practice

- ▶ Unusual system for users:
 - UI/UX?
 - Risk explanations

Social Secret Sharing: in Practice

- ▶ Unusual system for users:
 - UI/UX?
 - Risk explanations
- ▶ Displacement of the issue:
 - Trustees may not be trustworthy?

Social Secret Sharing: in Practice

- ▶ Unusual system for users:
 - UI/UX?
 - Risk explanations
- ▶ Displacement of the issue:
 - Trustees may not be trustworthy?
 - Not available?
 - Collusion

Conclusion

- ▶ CryptPad is a E2EE collaborative office suite
- ▶ And a bit more: calendars, teams...
- ▶ Aim at being user-friendly
- ▶ Future improvements:
 - Crypto-agility (\Rightarrow post-quantum secure collaboration)
 - Revocation
 - Conflict-free replicated data type
 - Proof of correct execution



cryptpad.org

- David - CryptPad Team Lead
- Daria - Junior Developer
- Diana - Junior Developer
- Fabrice - R&D Engineer
- Mathilde - Community & Support
- Wolfgang - R&D Engineer
- Yann - Privacy Engineer
- Zuzanna - Developer
- Ludovic - XWiki CEO

cryptpad.org

👉 Thank you for your attention. Questions?

Bibliography

-  I. S. Reed and G. Solomon.
Polynomial codes over certain finite fields.
In *J. Soc. Indus. Appl. Math.*, 1960
-  A. Shamir.
How to Share a Secret.
In *Communications of the ACM*, 1979