Securely collaborate with CryptPad

Fabrice Mouhartem
February 03, 2024
FOSDEM
CryptPad

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed et sapien euismod, dignissim nibh eget, rutrum odio. Sed at diam at nisl lacinia finibus.

Suspendisse sagittis ligula et convallis fermentum. Sed at diam at nisl lacinia finibus.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed et sapien euismod, dignissim nibh eget, rutrum odio. Sed at diam at nisl lacinia finibus.

Nullam tristique, urna et scelerisque interdum, turpis ante lacinia nisl, nec maximus lacus nisl sed metus.
Privacy-Friendly Collaborative Edition

Collaboration

Privacy

CryptPad

Yes, you can have both

Securely collaborate with CryptPad
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.
Blueprints

Cryptographic analysis & prepare for the future

Possible improvements:
- Cryptographic agility
- Password Recovery
- Revocation

Securely collaborate with CryptPad
Cryptographic analysis & prepare for the future

Possible improvements:
- Cryptographic agility
- Password Recovery
- Revocation
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

Secret secret

- c2Vw
- cmVo
- c2Ny

Securly collaborate with CryptPad
Social Secret Sharing: in Theory

- secret
- c2Vw
- cmV0
- c2Ny
- secret

Securely collaborate with CryptPad
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 (⇒ 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

Securely collaborate with CryptPad
cryptpad.org

👉 Thank you for your attention. Questions?
I. S. Reed and G. Solomon. 
*Polynomial codes over certain finite fields.* 

A. Shamir. 
*How to Share a Secret.* 
In *Communications of the ACM*, 1979