



CryptPad

The Future of CryptPad, an End-to-End
Encrypted Collaborative Office Suite

Fabrice Mouhartem

July 3rd, 2024. Pass the Salt, Lille

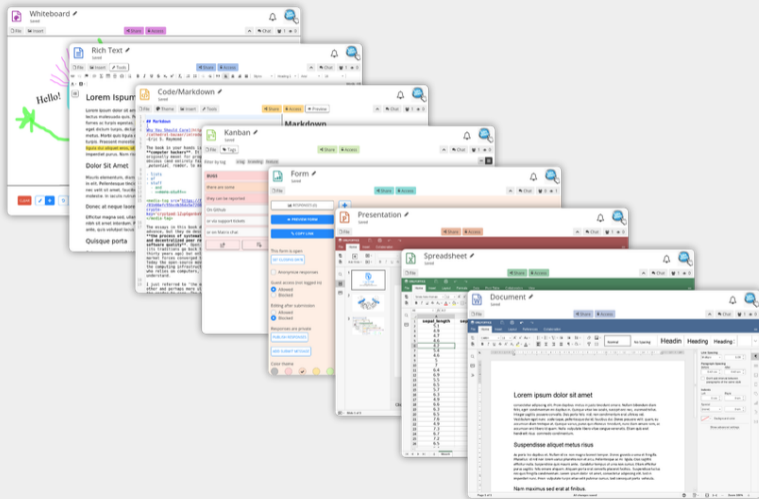
- ▶ End-to-End Encrypted

- ▶ End-to-End Encrypted
- ▶ Open-Source
 - Kerckhoffs' principle
 - AGPLv3

- ▶ End-to-End Encrypted
- ▶ Open-Source
 - Kerckhoffs' principle
 - AGPLv3
- ▶ Collaborative

- ▶ End-to-End Encrypted
- ▶ Open-Source
 - Kerckhoffs' principle
 - AGPLv3
- ▶ Collaborative
- ▶ Office Suite

CryptPad



CryptPad: A Collaborative Office Suite

The screenshot displays the CryptPad collaborative office suite interface. At the top, the document title is "Employees 2023" with a "Saved" status. The interface includes a "File" menu, "Share" and "Access" buttons, and a chat icon. The main workspace is a spreadsheet with the following data:

Employee ID	First Name	Last Name	Position	Start Date
1001	John	Doe	Software Engineer	1/15/2022
1002	Jane	Smith	Sales Associate	9/5/2021
1003	Michael	Johnson	HR Manager	3/10/2023
1004	Emily	Williams	Marketing Intern	6/20/2023
1005	Robert	Brown	Data Analyst	11/30/2022
1006	Sarah	Lee	Accountant	7/12/2021
1007	David	Kim	Project Manager	8/25/2022
1008	Olivia	Anderson	IT Technician	2/2/2023
1009	Ethan	Martinez	Sales Manager	12/18/2021
1010	Ava	Rodriguez	Graphic Designer	5/9/2022
1011	Liam	Hernandez	Customer Support	1/3/2023
1012	Mia	Davis	Operations Lead	6/22/2022
1013	Noah	Wilson	Marketing Manager	10/30/2021
1014	Sophia	Taylor	Software Developer	4/8/2023
1015	Benjamin	Anderson	HR Coordinator	9/14/2022
1016	Amelia	Moore	Data Scientist	11/12/2021
1017	James	Thomas	Sales Representative	7/5/2022
1018	Ella	Jackson	Financial Analyst	3/28/2023
1019	William	White	Marketing Coordinator	4/17/2022

The interface also features a rich text editor toolbar with options for font (Calibri), size (11), bold, italic, underline, text color, background color, and alignment. A right-hand sidebar provides settings for fill, borders, indent, text orientation, and text control. The bottom status bar shows "Sheet1" and "Zoom 100%".

CryptPad: A Collaborative Office Suite

The screenshot displays the CryptPad interface. At the top, a document titled "Lorem Ipsum" is shown as "Saved". The editor includes a toolbar with "File", "Insert", and "Tools" buttons, and "Share" and "Access" options. A rich text editor toolbar is visible below, with various text formatting icons and a "Styles" dropdown menu. The main text area contains a paragraph of Lorem Ipsum text, with several words highlighted in yellow. A "Contents" sidebar on the left lists document sections. On the right, a "Comments" panel shows a chat conversation with users "billy" and "george".


Contents

- Dolor sit amet
- Nulla facilisi
- Morbi maximus
- Nulla mollis
- Vestibulum nec fring...
- Praesent eget












Comments



- billy** 10/18/2023, 2:14:33 PM
Indeed
- george** 10/18/2023, 2:19:11 PM
Yes, I also agree with this!!
- george** 10/18/2023, 2:19:47 PM
- billy** What do you think?
- billy** 10/18/2023, 2:23:26 PM
I think we can rewrite that
Edited

CryptPad: A Collaborative Office Suite

Markdown doc 

Saved

 File  Theme  Insert  Tools  Share  Access  Preview  ^  Chat  1  0


 

```
1 # **Markdown**
2
3
4
5 [Wikipedia Markdown](http://https://en.wikipedia.org/wiki/Markdown)
6
7 Markdown is a lightweight markup language for creating formatted text using a
8 plain-text editor.
9 <media-tag
10 src="https://files.cryptpad.fr/blob/25/256fb38775bce8a9b03e23d63dc740b26ff7113a1e7
11 ffa21" data-crypto-key="cryptpad:gSo20E+9b1ksbKS+/0aJEAwS3XXqfc4Rnmv1TgtPGzQ=">
12 </media-tag>
13
14 > "to write using an easy-to-read and easy-to-write plain text format, optionally
15 convert it to structurally valid XHTML (or HTML)"
16
17
18 * Actually learn Markdown
19 * Write article
20   * Notes
21   * Examples
22
23
```

Markdown

[Wikipedia Markdown](#)

Markdown is a lightweight markup language for creating formatted text using a plain-text editor.



"to write using an easy-to-read and easy-to-write plain text format, optionally convert it to structurally valid XHTML (or HTML)"

- Actually learn Markdown
- Write article
 - Notes
 - Examples

CryptPad: A Collaborative Office Suite

 **Test slides** 
Saved  

File Theme Insert Tools Share Access Preview Present Chat 1 0

```
1 # Markdown
2
3
4 <media-tag
5   src="https://files.cryptpad.fr/blob/27/270359025ac58d111e8a1e96b29b4e18cc5e6c1468
6   1816e" data-crypto-key="cryptpad:fd100DmXo++nAGyL63GwUsJIXpG1Y\BL33QT+Y3oNTI=">
7 </media-tag>
```

Welcome to the **Test Markdown Slides** presentation! In this presentation, we will explore the power of [Markdown](https://en.wikipedia.org/wiki/Markdown) and its *ability to create beautiful and engaging slides.*

Markdown



Welcome to the **Test Markdown Slides** presentation! In this presentation, we will explore the power of [Markdown](#) and its *ability to create beautiful and engaging slides.*


CryptPad: A Collaborative Office Suite

The screenshot displays the CryptPad interface for a document titled "Vacation". The document is marked as "Saved". The top navigation bar includes "File" and "Insert" menus, along with "Share" and "Access" buttons. On the right, there are icons for a bell, a smiley face, and a chat window showing "0" messages and "1" viewer. The main canvas contains a drawing of a landscape with a yellow sun in the top right, a cyan sky, and a blue ground. The drawing tools at the bottom include a "CLEAR" button, a pencil icon, a plus sign, undo and redo buttons, a text tool, and a trash icon. The tool settings show "Width: 20px" and "Opacity: 100%". A color palette with 16 different colors is also visible.

CryptPad: A Collaborative Office Suite







The screenshot displays the CryptPad web application interface. At the top, the document title is "Random algorithm" with a "Saved" status. Navigation buttons for "File", "Share", and "Access" are visible. A menu bar includes "File", "Edit", "View", "Arrange", "Extras", and "Help". Below the menu is a toolbar with various editing tools. On the left, a "Scratchpad" panel contains a search bar and a "General" category with a grid of shapes. The main workspace features a flowchart diagram on a grid background. The diagram starts with a yellow rounded rectangle labeled "Start", followed by a yellow diamond decision box labeled "Is goal?". A "no" path leads to a stick figure labeled "Actor", and a "yes" path leads to a black circle. On the right, a "Style" panel is open, showing options for "View" (Grid, Page View), "Background" (Background Color, Shadow, Sketch), "Options" (Connection Arrows, Connection Points, Guides), and "Paper Size" (A4, Portrait, Landscape). Buttons for "Edit Data..." and "Clear Default Style" are at the bottom of the style panel.



CryptPad: A Collaborative Office Suite





Teambuilding activities-eng


Saved

 File  Share  Access  Chat  1  0

 RESPONSES (0) 


 PREVIEW FORM


 COPY PUBLIC LINK

 FORM SETTINGS



This form is open
Responses are private
[Guest access \(not logged in\)](#)
Allowed
[Submission](#)
One time and edit/delete


Color theme




 Description

Please take a moment to go through the following list of activities and indicate your preferences accordingly.
Keep in mind that **some activities might have limited spots**, so make sure to prioritize your top choices.





 EDIT  DELETE





 Choice ▾

What do you want to do?

Preview

- Nature Hiking 
- Scuba Diving 
- Campfire Bonding 
- Karaoke Party 

 EDIT  DELETE

CryptPad: A Collaborative Office Suite

The screenshot displays the CryptPad interface for a 'TODO july 2023' document. At the top left, there is a document icon and the title 'TODO july 2023' with a 'Saved' status and an edit icon. Below the title are 'File' and 'Tags' buttons. In the center, there are 'Share' and 'Access' buttons. On the right side, there is a notification bell, a smiley face icon, and a chat indicator showing '1' message and '0' views. Below the chat indicator is a minus sign and a menu icon.

The main content area features a Kanban board with three columns: 'To Do' (cyan), 'In progress' (yellow), and 'Done' (purple). Each column has a header with an edit icon and a plus sign button to the right of the 'Done' column. The 'To Do' column contains three tasks: 'Repair coffee machine' (priority), 'Call plumber' (priority), and 'Client meeting' (important). The 'In progress' column contains one task: 'Hire new intern' (hr). The 'Done' column contains two tasks: 'Create product documentation' (priority) and 'Organize office' (important). Each task card has an edit icon and a plus sign button below it. The board also includes filter tags 'hr', 'important', and 'priority' at the top left.

CryptPad: A Collaborative Office Suite

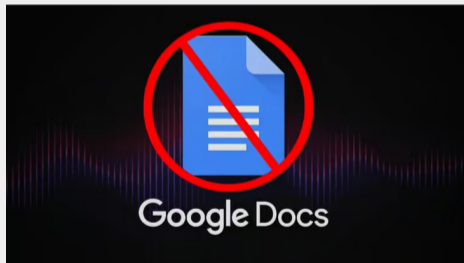
The screenshot displays the CryptPad Calendar interface for October 2023. The interface includes a sidebar on the left with a user profile 'billy' and several calendar categories: Appointments, Friends, My calendar, Vacation, Work, and New calendar. The main calendar grid shows events for each day of the month. The events are as follows:

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
25	26	27	28	29	30 Ibiza trip	1
2 Ibiza trip	3	4	5	6	7	8
9	10 Marketing meeting Doctor appointment	11	12 Michael's birthday	13 Presentation Day	14 National Holiday	15
16	17 Free day from work	18	19 Review Day	20	21	22
23 Coffee with Marie	24	25 Football game Blood test	26	27	28 Camping	29
30 Camping	31	1	2	3	4	5

TECH

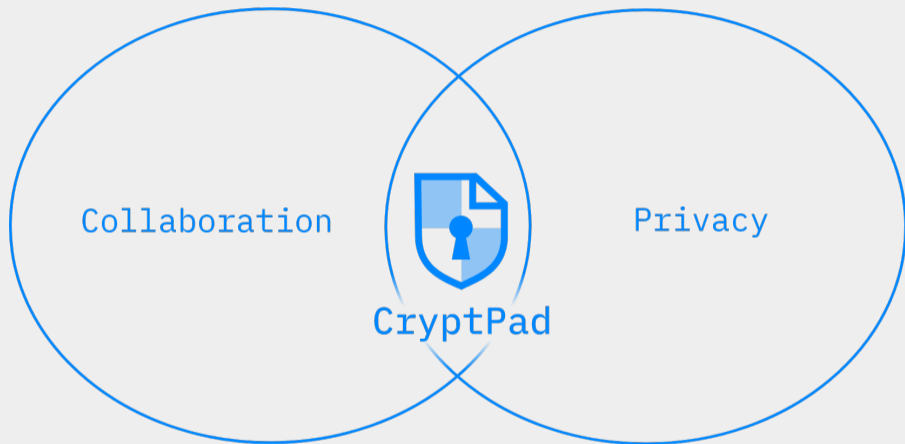
Romance author gets locked out of Google Docs for “inappropriate” content

Anurag Singh | Published: May 30, 2024, 12:06



<https://www.dexerto.com/tech/romance-author-gets-locked-out-of-google-docs-for-inappropriate-content-2713004/>

Collaboration and Privacy



Yes, you can have both

CryptPad offers:

- ▶ Pseudonymity of users
- ▶ Protection of pads' content and metadata

CryptPad offers:

- ▶ Pseudonymity of users
- ▶ Protection of pads' content and metadata
- ▶ Easy to use interface
- ▶ Accessibility

How CryptPad Works

Logging in

Login + Passphrase \xrightarrow{KDF} Keys

- ▶ Identifier: a public verification key

How CryptPad Works

Logging in

Login + Passphrase \xrightarrow{KDF} Keys

- ▶ Identifier: a public verification key
- ⇒ No link username ↔ public key

How CryptPad Works

Logging in

Login + Passphrase \xrightarrow{KDF} Keys

- ▶ Identifier: a public verification key
- ⇒ No link username ↔ public key
- ⇒ No password recovery

Security

Encrypted services Apple, Proton and Wire helped Spanish police identify activist

Lorenzo Franceschi-Bicchieri / 12:38 PM PDT • May 8, 2024

Comment



techcrunch.com/2024/05/08/encrypted-services-apple-proton-and-wire-helped-spanish-police-identify-activist/

CryptPad = Crypt + Pad

Historically

CryptPad = Encrypted Etherpad

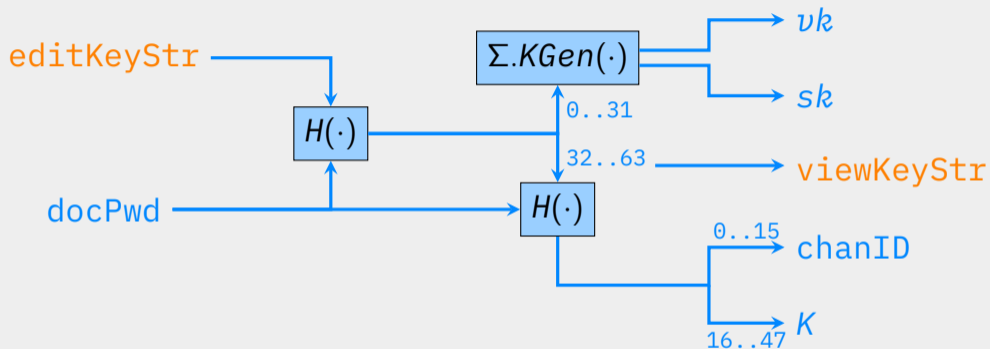
CryptPad = Crypt + Pad

Historically

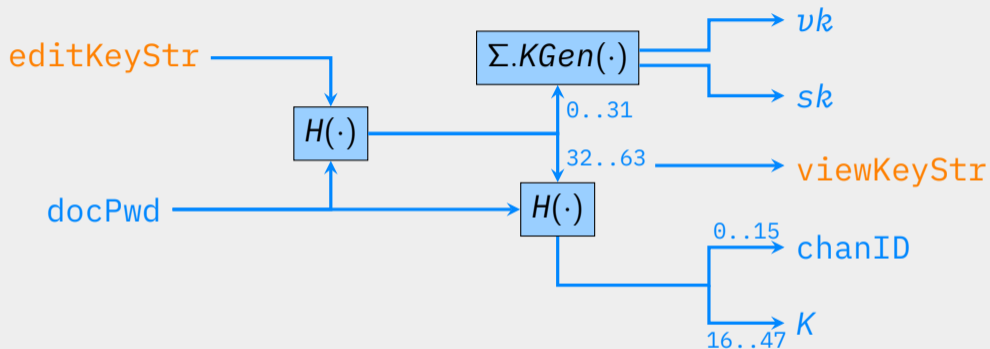
CryptPad = Encrypted Etherpad

- ▶ An editable computer file is often a text file
- ⇒ Collaborative edition can be generalised to multiple document types

Document Security



Document Security



- ▶ [https://cryptpad.fr/pad/#/2/pad/edit/\[editKeyStr\]/](https://cryptpad.fr/pad/#/2/pad/edit/[editKeyStr]/)
- ▶ [https://cryptpad.fr/doc/#/2/doc/view/\[viewKeyStr\]/](https://cryptpad.fr/doc/#/2/doc/view/[viewKeyStr]/)

So Far

- ▶ Built around cryptography

- Encryption

- Signatures

- Hash Functions

⇒ Secure by design

So Far

- ▶ Built around cryptography
 - Encryption
 - Signatures
 - Hash Functions
- ⇒ Secure by design
- ▶ With some limitations...
 - Password recovery

So Far

- ▶ Built around cryptography

 - Encryption

 - Signatures

 - Hash Functions

⇒ Secure by design

- ▶ With some limitations...

 - Password recovery

 - Revocation

So Far

- ▶ Built around cryptography

- Encryption

- Signatures

- Hash Functions

⇒ Secure by design

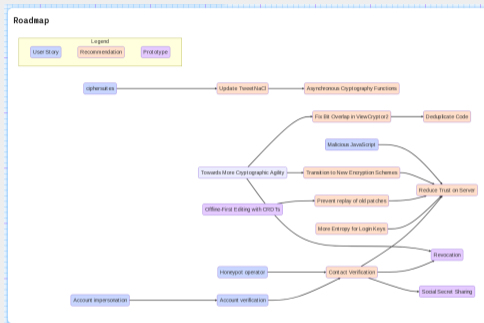
- ▶ With some limitations...

- Password recovery

- Revocation

- Strong trust on the server

Blueprints



▶ Security and usability analysis for CryptPad



<https://blueprints.cryptpad.org/>

Multiple resources:

- ▶ User-story based analysis



<https://blueprints.cryptpad.org/>

Multiple resources:

- ▶ User-story based analysis
- ▶ A whitepaper



<https://blueprints.cryptpad.org/>

Multiple resources:

- ▶ User-story based analysis
- ▶ A whitepaper
- ▶ Good practices: a blog post
 - Threat model



<https://blueprints.cryptpad.org/>

Multiple resources:

- ▶ User-story based analysis
- ▶ A whitepaper
- ▶ Good practices: a blog post
 - Threat model
- ▶ Prototypes

Threat Model

Instance Admin (*us*)

Honest but Curious

- ▶ Especially to deliver the correct code

Threat Model

Instance Admin (*us*)

Honest but Curious

- ▶ Especially to deliver the correct code

Collaborators

Honest but Curious

Threat Model

Instance Admin (*us*)

Honest but Curious

- ▶ Especially to deliver the correct code

Collaborators

Honest but Curious

Adversaries

Active adversary

Blueprints Prototype: Password Recovery

CryptPad: Recall

- ▶ No password storage on server
- ▶ No link between user public key and password

Blueprints Prototype: Password Recovery

CryptPad: Recall

- ▶ No password storage on server
- ▶ No link between user public key and password

⇒ How to safely store the password?

Blueprints Prototype: Password Recovery

CryptPad: Recall

- ▶ No password storage on server
- ▶ No link between user public key and password

⇒ How to safely store the password?

Issue

The cryptography-based design is a blocker

Blueprints Prototype: Password Recovery

CryptPad: Recall

- ▶ No password storage on server
- ▶ No link between user public key and password

⇒ How to safely store the password?

Issue

The cryptography-based design is a blocker

Solution: Use more cryptography!

Secret Sharing

t -out-of- n Secret Sharing

Coined by [RS60, Bla79, Sha79]:

- ▶ A secret S is split in n shards
- ▶ t shards are needed to reconstruct S

Secret Sharing

t-out-of-*n* Secret Sharing

Coined by [RS60, Bla79, Sha79]:

- ▶ A secret S is split in n shards
- ▶ t shards are needed to reconstruct S

- ▶ Information-theoretic secure

Secret Sharing

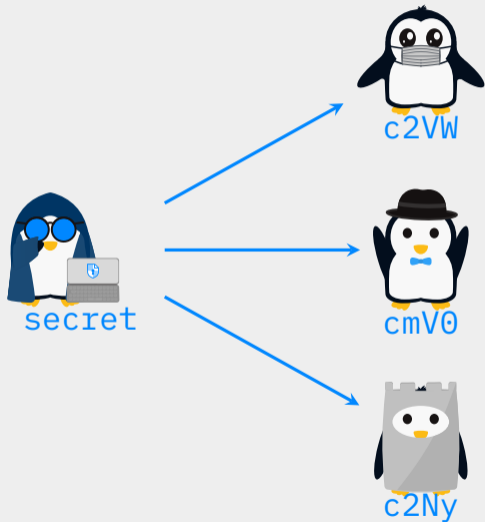
t -out-of- n Secret Sharing

Coined by [RS60, Bla79, Sha79]:

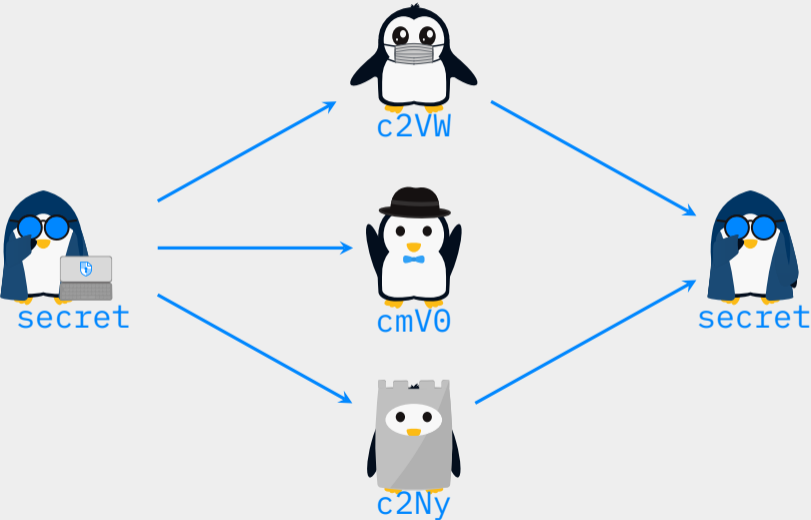
- ▶ A secret S is split in n shards
- ▶ t shards are needed to reconstruct S

- ▶ Information-theoretic secure
- ▶ Used in threshold-cryptography
- ▶ Used in some electronic voting schemes

Social Secret Sharing



Social Secret Sharing



Social Secret Sharing in CryptPad?

Core Idea

Share your **private keys** to **trustworthy** contacts

Social Secret Sharing in CryptPad?

Core Idea

Share your **private keys** to **trustworthy** contacts

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

Social Secret Sharing in CryptPad?

Core Idea

Share your **private keys** to **trustworthy** contacts

- ▶ Unconventional system for users:
 - UI/UX?
 - Risk explanations
- ▶ Displacement of the risk:
 - Trustees may not be **trustworthy**...

Social Secret Sharing in CryptPad?

Core Idea

Share your **private keys** to **trustworthy** contacts

- ▶ Unconventional system for users:
 - UI/UX?
 - Risk explanations
- ▶ Displacement of the risk:
 - Trustees may not be **trustworthy**...
 - Collusion

Social Secret Sharing in CryptPad?

Core Idea

Share your **private keys** to **trustworthy** contacts

- ▶ Unconventional system for users:
 - UI/UX?
 - Risk explanations
- ▶ Displacement of the risk:
 - Trustees may not be **trustworthy**...
 - Collusion
 - Not available?

Other Prototypes

- ▶ Revocation

- ▶ Offline-first editing

Other Prototypes

- ▶ Revocation

- Now: duplicate the file with the updated accesses

- ▶ Offline-first editing

Other Prototypes

- ▶ Revocation
 - Now: duplicate the file with the updated accesses
 - Introducing key rotation
 - A step toward forward-secrecy
- ▶ Offline-first editing

Other Prototypes

▶ Revocation

- Now: duplicate the file with the updated accesses
- Introducing key rotation
- A step toward forward-secrecy

▶ Offline-first editing

- Now: when offline, CryptPad switches to R0-mode

Other Prototypes

▶ Revocation

- Now: duplicate the file with the updated accesses
- Introducing key rotation
- A step toward forward-secrecy

▶ Offline-first editing

- Now: when offline, CryptPad switches to R0-mode
- Using conflict-free replicated data types (CRDTs)
- Prototype using Yjs

Conclusion

- ▶ CryptPad is an E2EE collaborative office suite
- ▶ Specific collaboration tools: calendars, teams...
- ▶ Aims at making cryptography accessible to all

Conclusion

- ▶ CryptPad is an E2EE collaborative office suite
- ▶ Specific collaboration tools: calendars, teams...
- ▶ Aims at making cryptography accessible to all
- ▶ Future works:
 - Integrating aforementioned prototypes

Conclusion

- ▶ CryptPad is an E2EE collaborative office suite
- ▶ Specific collaboration tools: calendars, teams...
- ▶ Aims at making cryptography accessible to all
- ▶ Future works:
 - Integrating aforementioned prototypes
 - Keep users informed with the Blueprints website

Conclusion

- ▶ CryptPad is an E2EE collaborative office suite
- ▶ Specific collaboration tools: calendars, teams...
- ▶ Aims at making cryptography accessible to all

- ▶ Future works:
 - Integrating aforementioned prototypes
 - Keep users informed with the Blueprints website
 - Crypto-agility (\Rightarrow toward post-quantum security)

Conclusion

- ▶ CryptPad is an E2EE collaborative office suite
- ▶ Specific collaboration tools: calendars, teams...
- ▶ Aims at making cryptography accessible to all
- ▶ Future works:
 - Integrating aforementioned prototypes
 - Keep users informed with the Blueprints website
 - Crypto-agility (\Rightarrow toward post-quantum security)
 - Less trust on the server: proof of correct execution?
 - Less trust on the browser: dedicated client?
 - Mobile application

cryptpad.org

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

cryptpad.org

👉 Thank you for your attention. Questions?

References

-  I. S. Reed and G. Solomon.
Polynomial codes over certain finite fields.
In *J. Soc. Indus. Appl. Math.*, 1960
-  G. Blakley.
Safeguarding cryptographic keys.
In Proc. of the National Computer Conference, 1979
-  A. Shamir.
How to Share a Secret.
In *Communications of the ACM*, 1979
-  Pingus: <https://github.com/EagleoutIce/tikzpingus>