

Capsule:
A Protocol for
Secure
Collaborative
Document Editing

Nadim Kobeissi



The screenshot shows a web browser window with a single tab titled "Very Secret Document - Google". The address bar contains the URL "https://docs.google.com/document/d/1DcOuK0xi...". The document title is "Very Secret Document" and it is marked as "All changes saved in Drive". The toolbar includes options for File, Edit, View, Insert, Format, Tools, Add-ons, and Help. The text "Plan to conquer the world" is centered on the page in a large, black, sans-serif font. The status bar at the bottom shows "PAGE 1 OF 1", "4 WORDS", and "ENGLISH (US)".

The screenshot shows a web browser window with a single tab titled "Document.docx - Microsoft Word". The address bar contains the URL "https://onedrive.live.com/edit.aspx?resid=B71DD...". The document title is "Document.docx" and it is marked as "Saved to OneDrive". The interface includes a ribbon with tabs for FILE, HOME, INSERT, PAGE LAYOUT, REVIEW, VIEW, and EDIT IN WORD. The text "Very sensitive work plans" is centered on the page in a blue, sans-serif font. The status bar at the bottom shows "PAGE 1 OF 1", "4 WORDS", "ENGLISH (US)", and "100%".

| Capsule:
Security Goals

Participant List Integrity.

Confidentiality.

Integrity.

Authentication.

Transcript Consistency.

Capsule: Simple, Elegant Protocol

- Document is a *hash chain of diffs*.
- Access to document is obtained by sharing a simple ID.
- Users must prove knowledge of ID to participate in document.
- Primitives:
 - BLAKE2 for symmetric operations.
 - Ed25519 for signatures.

Capsule: Formally Verified

Protocol Level

- Formally verified with ProVerif.
- Hand proof.

Implementation Level:

- HACL-WASM: First software to use HACL* in WebAssembly.
- Functional correctness, secure memory, no side channels.

Capsule: Amazing!

- An open standard that anyone can use.
- Learn more: <https://symbolic.software/capsule/>
- ePrint paper: <https://eprint.iacr.org/2018/253>