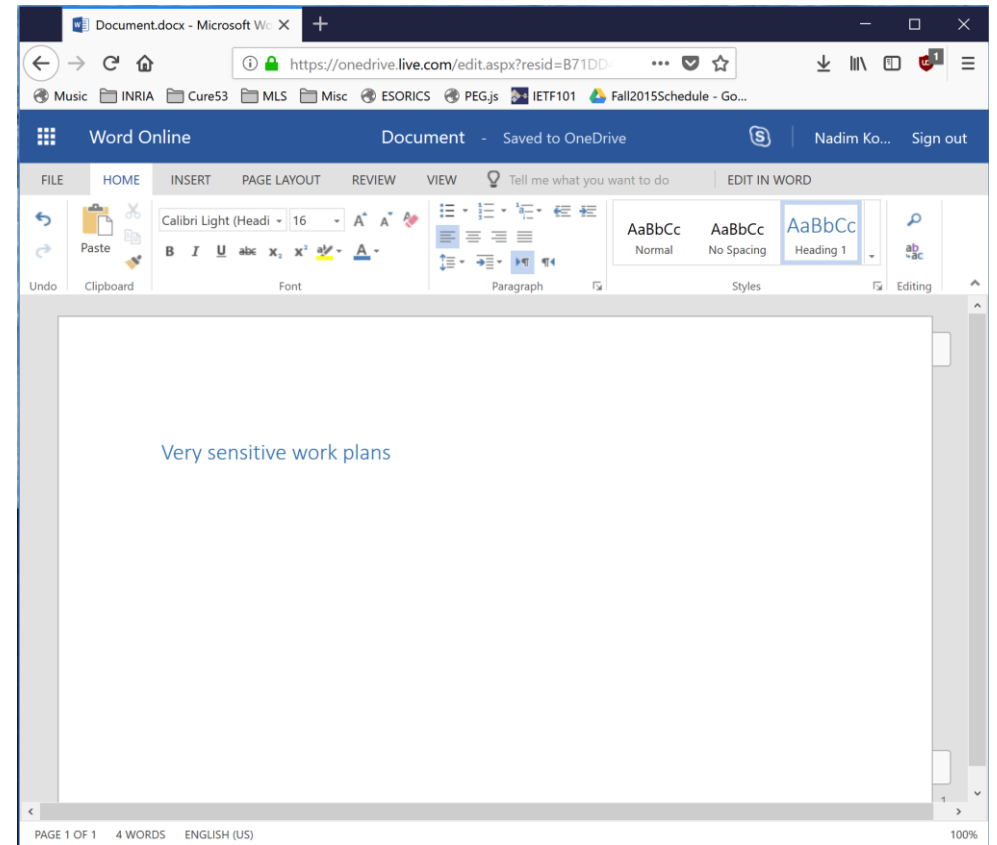
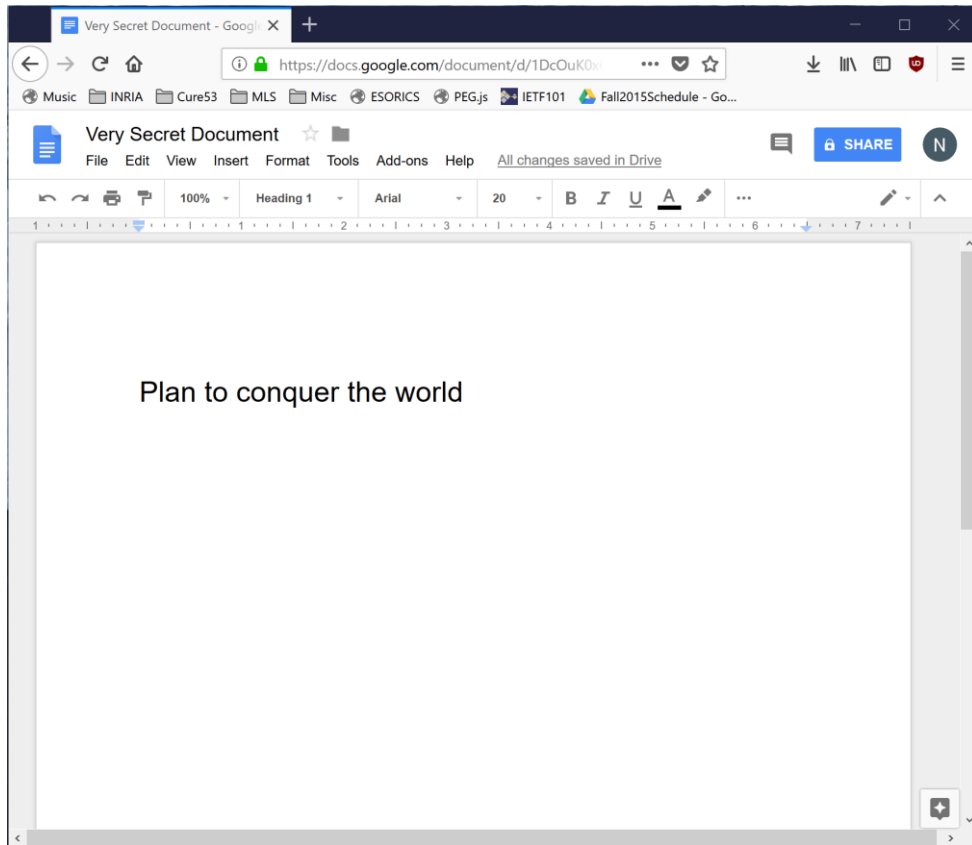


Capsule:
A Protocol for
Secure
Collaborative
Document Editing

Nadim Kobeissi





We've all been there...

| 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>
- Email me! nadim@symbolic.software