6-May:

1. How would you introduce the idea of formal verification to students?

Obj is to expand on previous work
→ qRHL quick-start guide

Formal Verification: A primer.

---

2. Discuss about setting up the environment.

→ Screen recording + Audio?

→ Script that can do the install.

→ Zulip: There will be a distributable in the first release

---

3. Recommended pre-requisites.

---

4. Formal logics and abstraction.: Introduction.

5. Idea : PDF + .ec files demonstrating certain concepts? ?
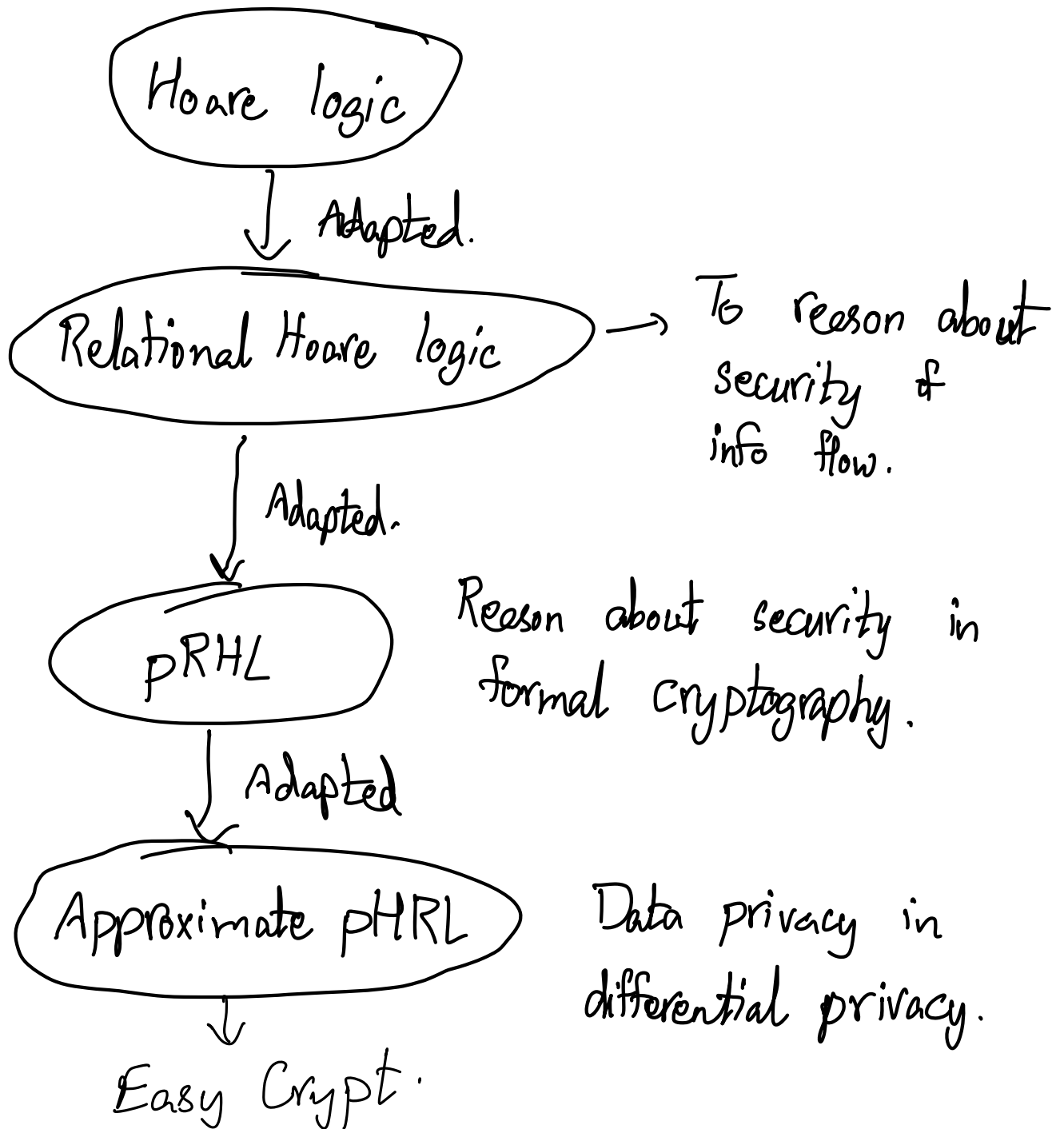
6. chap 0 is a good way to demonstrate ambient logic.

7. Various models of formal verification. ← In preface.
   └→ Draw from the stackoverflow answer, galois blogpost and discuss with Dominique

8. Logic:

Hoare logic

↓ Adapted.

Relational Hoare logic → To reason about security of info flow.

↓ Adapted.

PRHL

Reason about security in formal cryptography.

↓ Adapted

Approximate pHRL

Data privacy in differential privacy.

↓

Easy Crypt.

Trying to trace what EasyCrypt is built on.

Can we discuss Coq and other tools: To get a fair picture.