Vanishing Database + Turtl

Hal Triedman
Professor Seny Kamara

For my project, I attempted to change one specific cryptographic facet of Turtl, an open-source encrypted collaborative notes app used by Brown University's Transformative Justice (TJ) program, and which may expose the program to legal liability. The TJ program deals with issues that may be legally sensitive, and as such it needs a document-sharing program that is immune to subpoenas. Encrypted notes, if stored on the database in perpetuity, may be vulnerable to subpoenas, exposing the program and participants in it to legal liability. To help combat that liability, I worked on integrating a "vanishing database" (vdb) API, created by Professor Seny Kamara and graduate students Ghous Amjad and Lucy Qin, into Turtl. The vdb uses searchable encryption to make document keys encrypted and retrievable, and also uses Neuralyzer to allow for enforceable expiration dates on keys. Though it doesn't completely remove legal liability (i.e. participants in the TJ program could copy notes/files or a subpoena could be served before notes have expired), it begins to close off the subpoena vulnerability.

I ended up creating a new fork of Turtl and editing some of the key internal functions on several parts of the app. That code, which is my project artifact, is available on Github.