

# Crypto-Book: Privacy Preserving Online Identities



John Maheswaran, David Isaac Wolinsky, Bryan Ford  
Department of Computer Science, Yale University



[www.crypto-book.com](http://www.crypto-book.com)

## I. Overview

Cross-site authentication schemes mean users rely on social networking sites for their digital identities

Use of these identities brings privacy/tracking risks

We propose **Crypto-Book**

- extension to existing digital identity infrastructures
- offers privacy-preserving, digital identities
- uses *anytrust* servers [Wolinsky *et al.* EuroSec'12]
  - assign key pairs to a social identity
  - requires only one honest server for safety



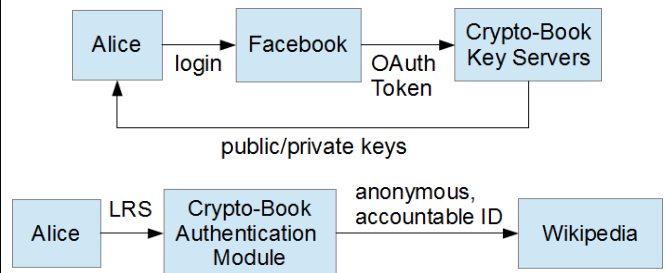
## II. Example Use Case

Alice wants to anonymously edit Wikipedia

Wikipedia thinks anonymous edits lead to vandalism

Crypto-Book provides an **anonymous, accountable ID** for Alice to log into Wikipedia

Wikipedia can block Alice's ID without deanonymizing her

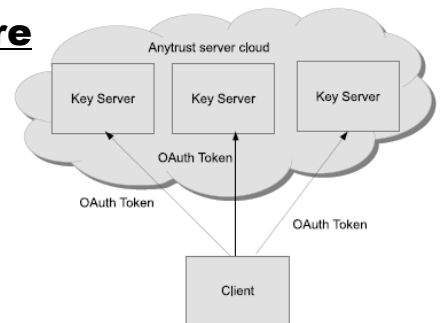


## III. Our Architecture

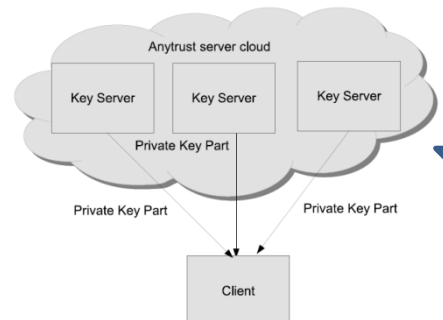


**Step 1:** Client authenticates with Facebook

Goal	Strategy
Usable	Build on top of existing social networks
Resist dishonest key servers	Use anytrust cloud to <i>split trust</i> across servers
Privacy protecting	LRS cryptographically anonymizes users
Accountability	LRS ensures 1-to-1 mapping
Modular	Could easily use alternative <ul style="list-style-type: none"> <li>• key assignment</li> <li>• anonymizing crypto</li> </ul>



**Step 2:** Client sends OAuth token



**Step 3:** Key servers send private key to client

**Step 4:** Client makes linkable ring signature (LRS) with keys to authenticate to third parties