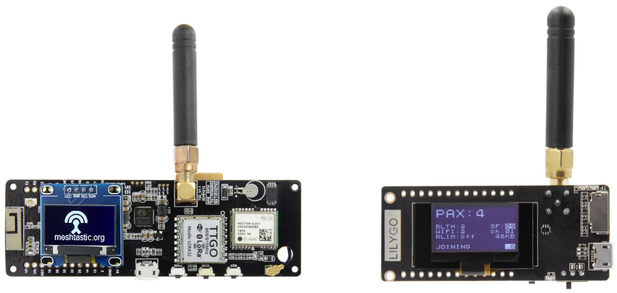
Black Lager: A Secure Radio Mesh Text Messaging App

Developed by Ahmed Kaddoura, Josh Li, Matyas Krizek, and Mike Zhao
Sponsored by Paul Lambert

UNIVERSITY OF SAN FRANCISCO

A text messaging application that runs without cell service or internet. Data is sent over a mesh network of small, power-efficient, inexpensive long-range radios. Messages are authenticated with lightweight public key certificates and digital signatures. Built on top of Meshtastic open source software that forms an off-grid, decentralized, mesh network.



Long-Range Radio Hardware

LoRa radio devices make up a mesh network of up to 80 nodes. When a receiving node captures a packet, it rebroadcasts it to the other nodes in range. Packets are sent over the 915 MHz unlicensed radio band. The devices are low-power ESP32 microcontrollers flashed with the application firmware that connect through USB to a computer running the Python application. Implemented and tested using LILYGO Lora v2.1 and T-Beam devices that cost less than $30.

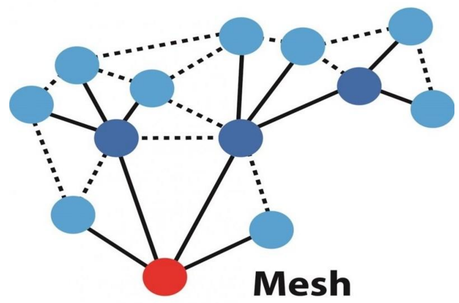
Public Key Certificates

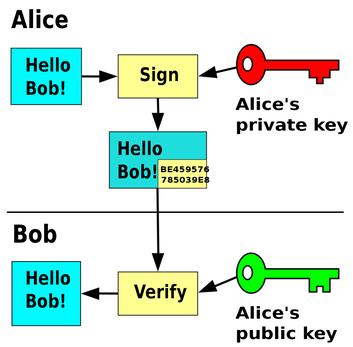
Lightweight public-key certificates and digital signatures with the Ed25519 algorithm.

Generate a persona with a name and public/private key pair using the Python application.

Send and verify signed text messages with owned and peer personas stored on the client-side.

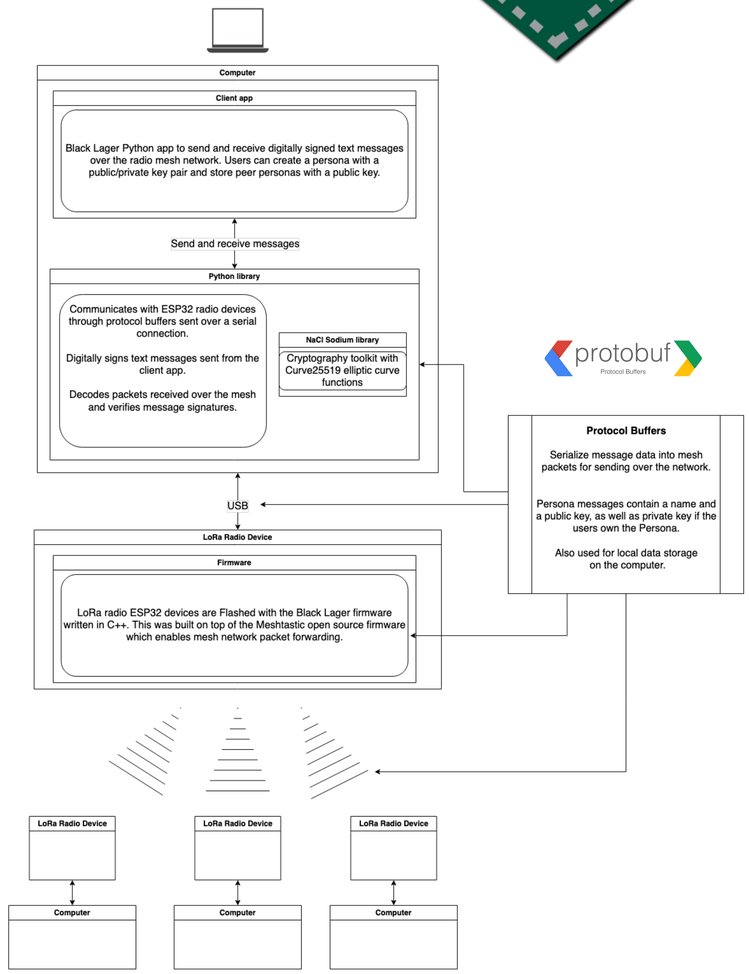
Digital signature scheme uses SHA-512 hashing and Curve25519 elliptic-curve cryptography.





The public key certificates and corresponding Python library implemented provide message authentication and can be extended for further security enhancements. Implementing the Elliptic-curve Diffie-Hellman key agreement protocol would allow two users to compute a shared secret key to use in symmetric encryption of text messages. A possible limitation is US government regulation on cryptography.

black-lager.github.io



Black Lager can be used for secure emergency communications, for example during earthquakes, when cell service and internet are unavailable to communicate with responding agencies like the Red Cross. The firmware is also interoperable with the Meshtastic iOS and Android clients which can be used to send unsigned messages by connecting a phone to a radio via Bluetooth.

python™ libsodium C++ LoRa®