Chapter 1. Introduction

https://katzenpost.network/blog/2024-04-12-hpqc/

"hpqc - hybrid post quantum cryptography library"

(and other things in this blog)

• Why is this the right tool for me? • Most advanced (PD hybrid) crypto, best anonymity, best mixnet protocols.

• The Noise Protocol Framework is used end to end in KP., in place of TLS. Too much tech debt. Much simpler and better integrated overlay network.

• Threat model document has a one page summeary – use it in the admin guide. Currently in blogpost section.

Router defniton: creates ingress and egress queues. KP adds of crytptographui between. Ques with thread pools in between, capable of dynamically dropping packets based.

Client2 – description of the protocol should be drawn from the paper. Minimal history about advancements over Loopix.

- There are old and new protocols. Katzen currently supports only the old protocol. What is this referring to? Loopix is the old protocol. Poor anonymity because direct connections are observable. Typical of the disconnect between academic s and the real world desired features. The choose the wrong threat model.
- The new protocol has durable streams

OLD

Katzenpost can be used as a message oriented transport for a variety of applications and is in no way limited to the e-mail use case demonstrated by the `mailproxy` client/library. Other possible applications of Katzenpost include but are not limited to: instant messenger applications, crypto currency transaction transport, bulletin board systems, file sharing and so forth.

Insert somewhere:

Example 1.1.

<caption>dawuud1:56 PM [https://bench.cr.yp.to:41867/research/pl/mjgbpzht4pdympsqbcmfudcxoe]

@jdormansteele we should mention somewhere in the server side documentation that ALL katzenpost mixnets have packet loss during startup because mix nodes accept connections before they've connected outbound, so when they receive packets they get dropped since there is nowhere to send them.
</caption>

***** Mine the academic paper *****