Problem

Stateless Reset is indistinguishable from a QUIC packet
... that no one can decrypt

Stateless Reset is send in response to a QUIC packet
... than an endpoint can’t decrypt
There is only one thing that stops the resulting exchange:
There is no amplification, so packet loss ends it
Simple Solution

Stateless Reset is small

Don’t send it if it is smaller than the packet that was received

It isn’t the smallest possible packet though

So really small packets never trigger a stateless reset
Slightly More Complex Solution

Randomly drop stateless reset if it isn’t smaller than the incoming packet

For example,

\[ P(\text{ignore}) = \text{len(reset)} > \text{len(packet)} \]

might become

\[ P(\text{ignore}) = (\text{len(reset)} - \text{len(packet)} + A) / B \]