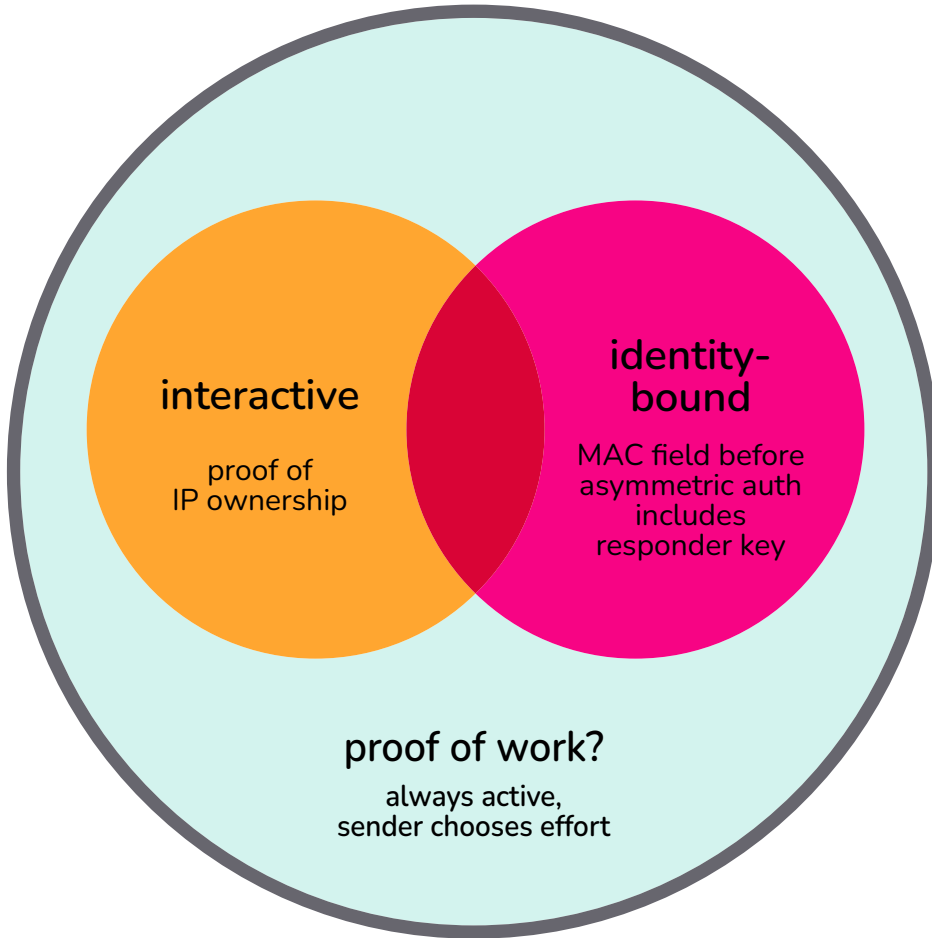


# Knock Patterns



**all knock patterns**

**allowed patterns**

must be global to the protocol  
(no peer-bound information)

choice to use must be made by initiator

**minimize!**

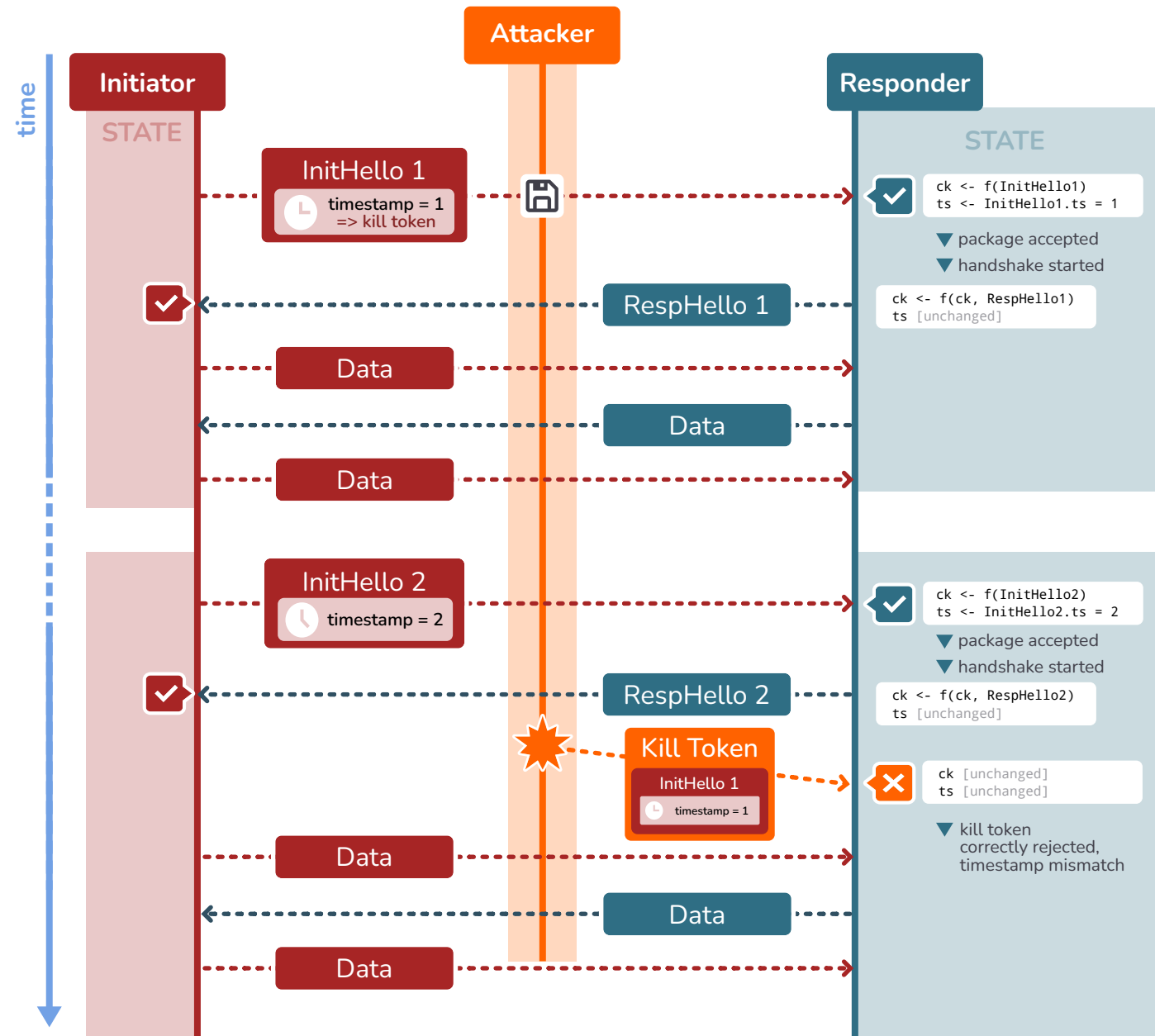
breaks  
stealth

**never use!**

breaks  
identity  
hiding

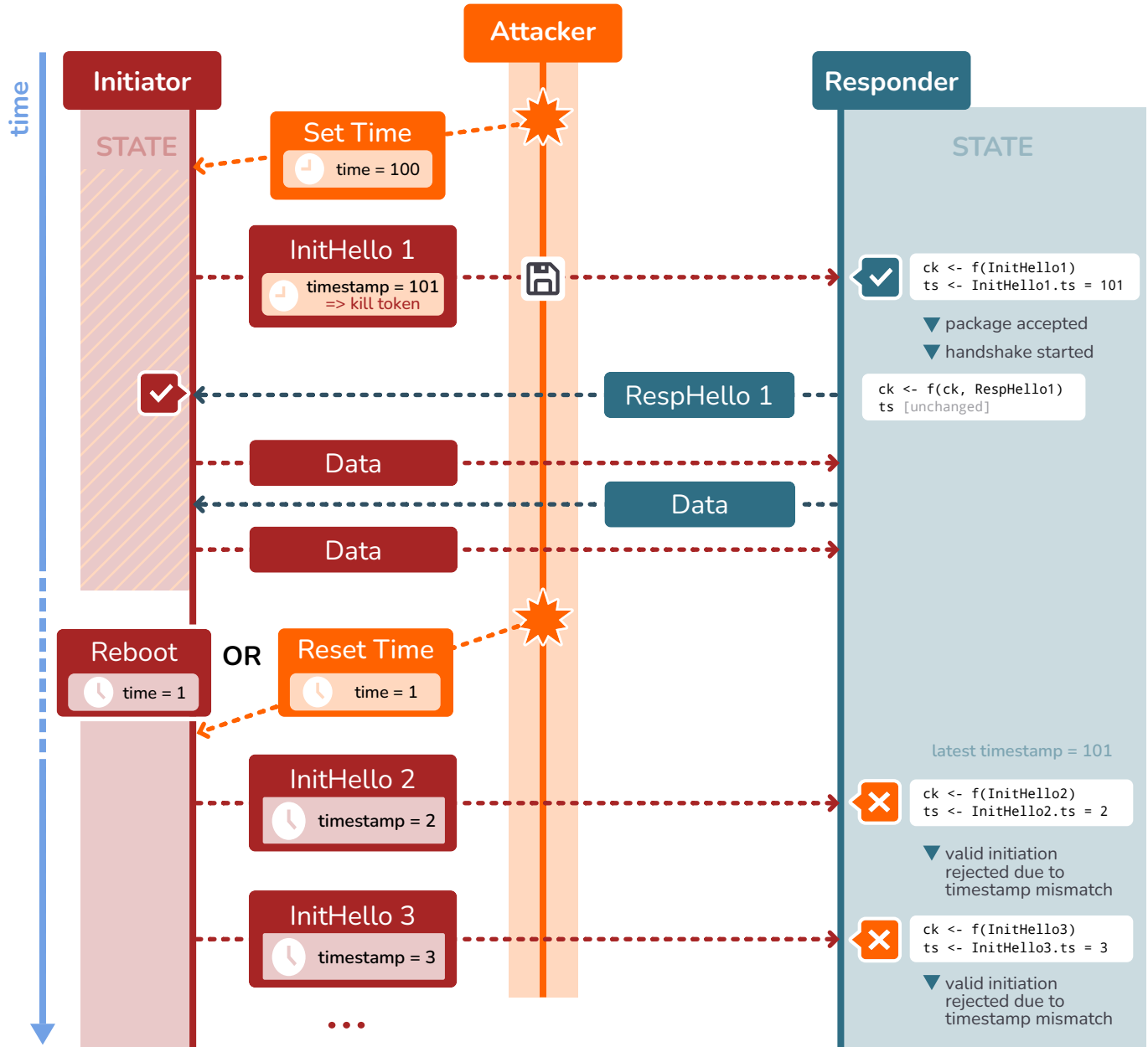
# WireGuard Retransmission Protection

intended function



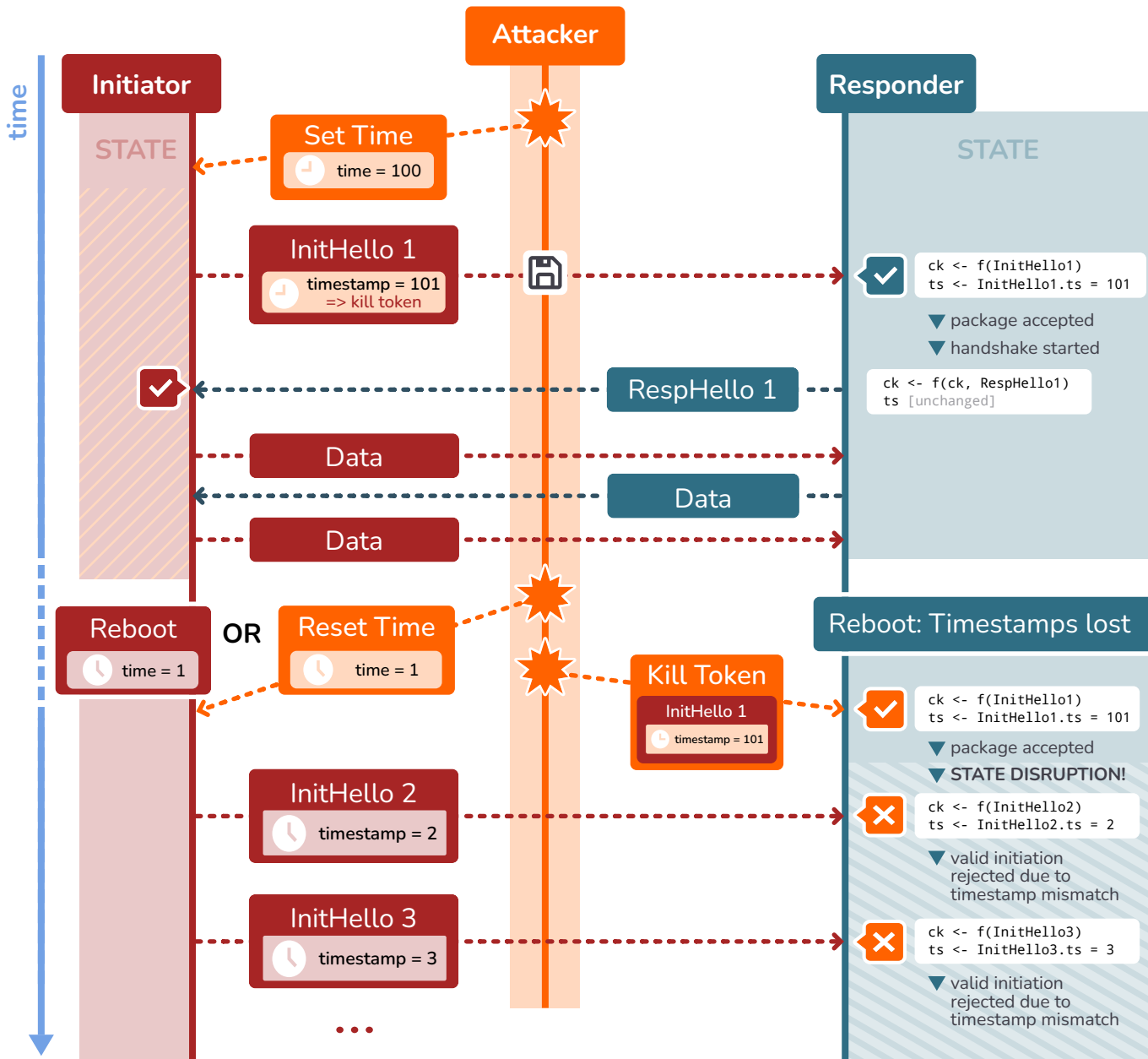
# ChronoTrigger attack against WireGuard – Immediate Execution

state disruption attack against WireGuard based on the insecurity of the Network Time Protocol

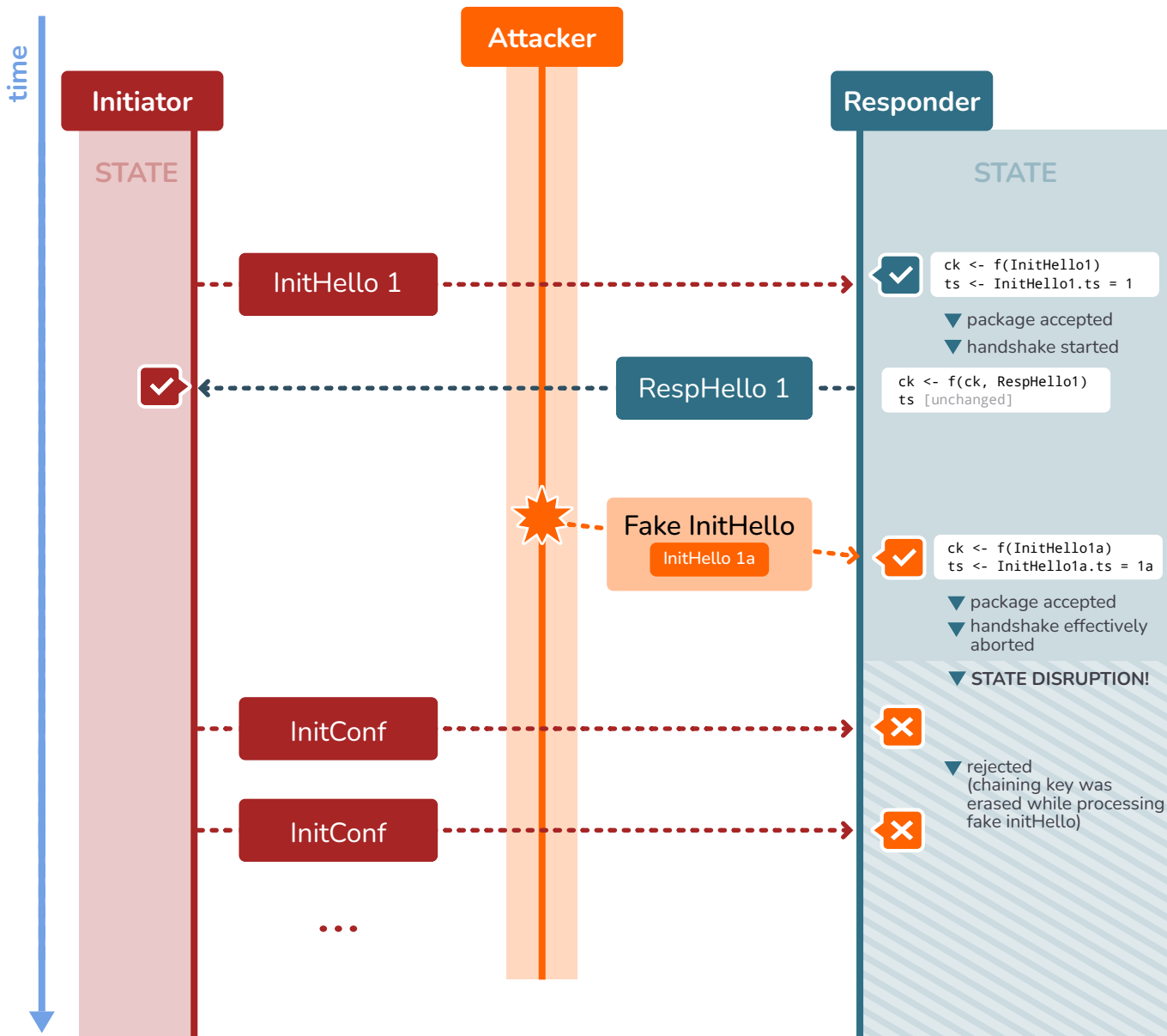


# ChronoTrigger attack against WireGuard – Delayed Execution

state disruption attack against WireGuard based on the insecurity of the Network Time Protocol

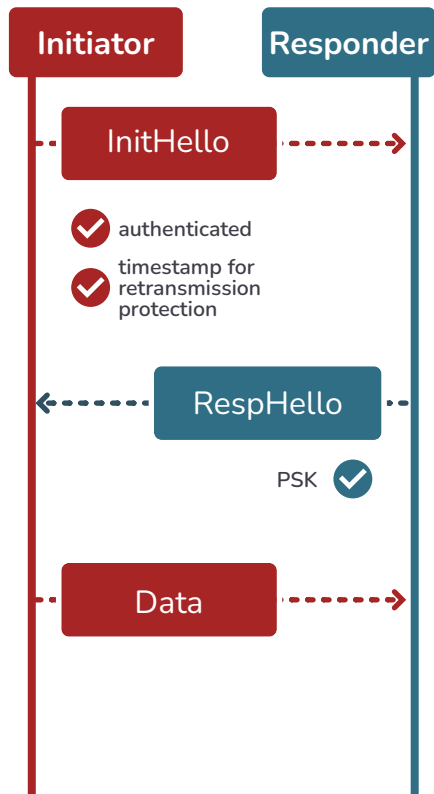


# Post-Quantum WireGuard allows state disruption since InitHello is unauthenticated



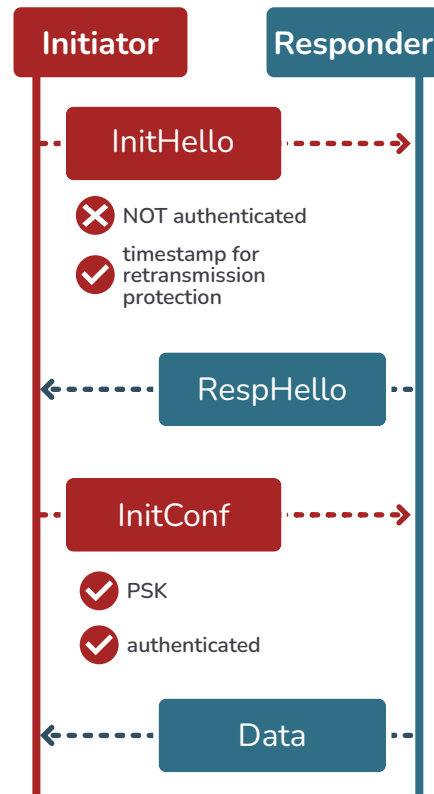
# Post-Quantum WireGuard allows state disruption since InitHello is unauthenticated

## WireGuard



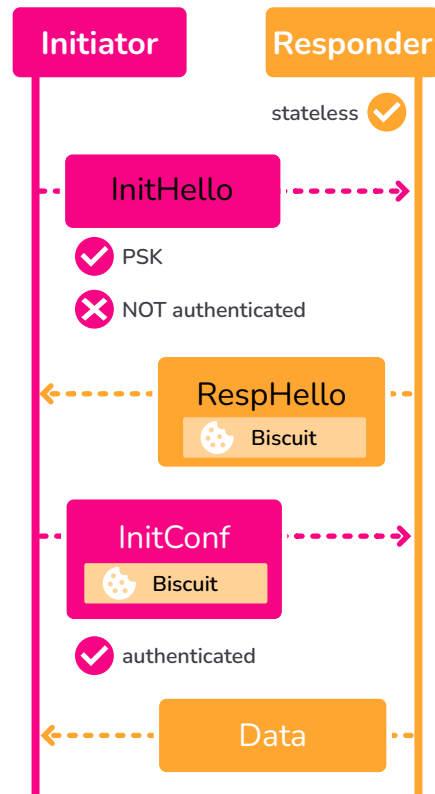
 **Susceptible to ChronoTrigger**

## Post-Quantum WireGuard



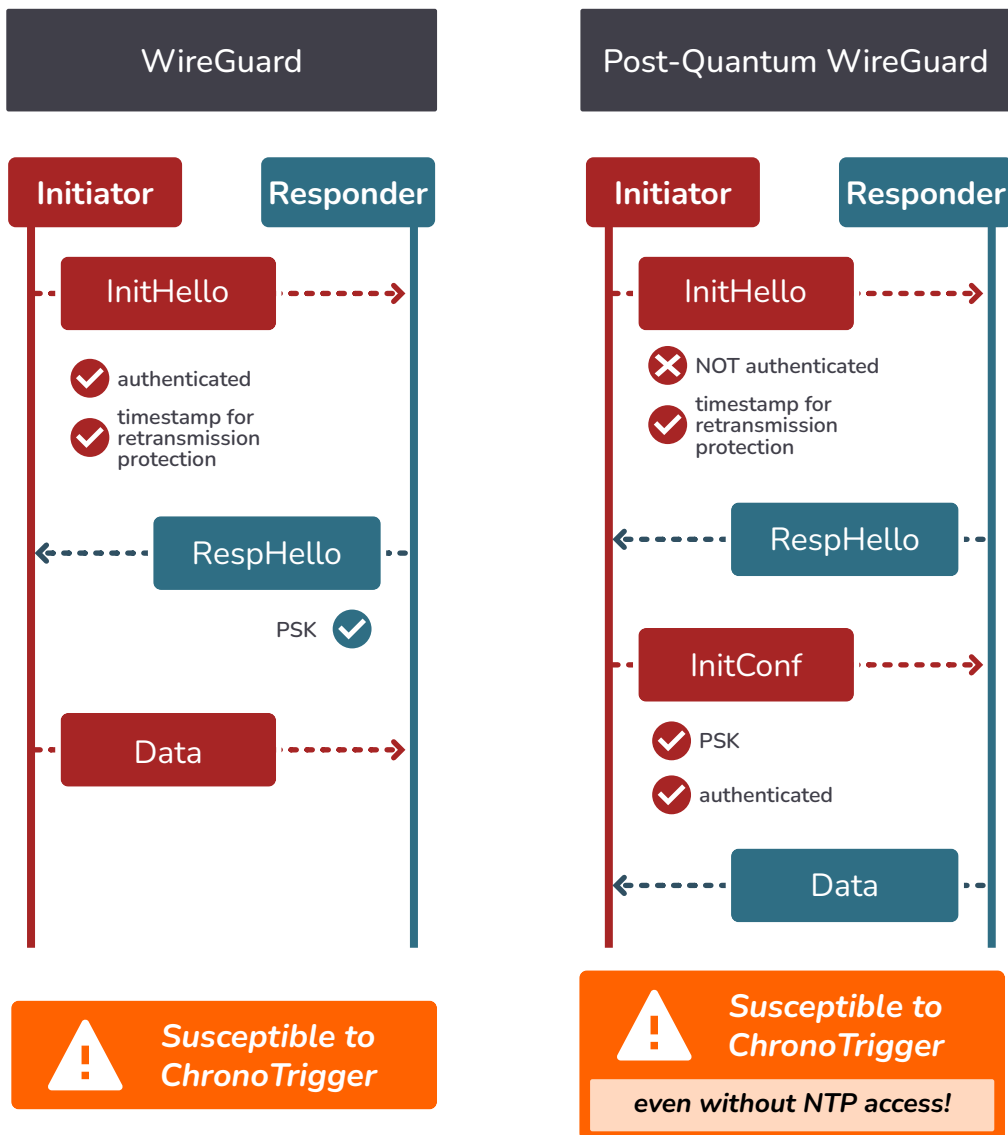
 **Susceptible to ChronoTrigger**  
even without NTP access!

## Rosenpass



**Not susceptible due to stateless responder**

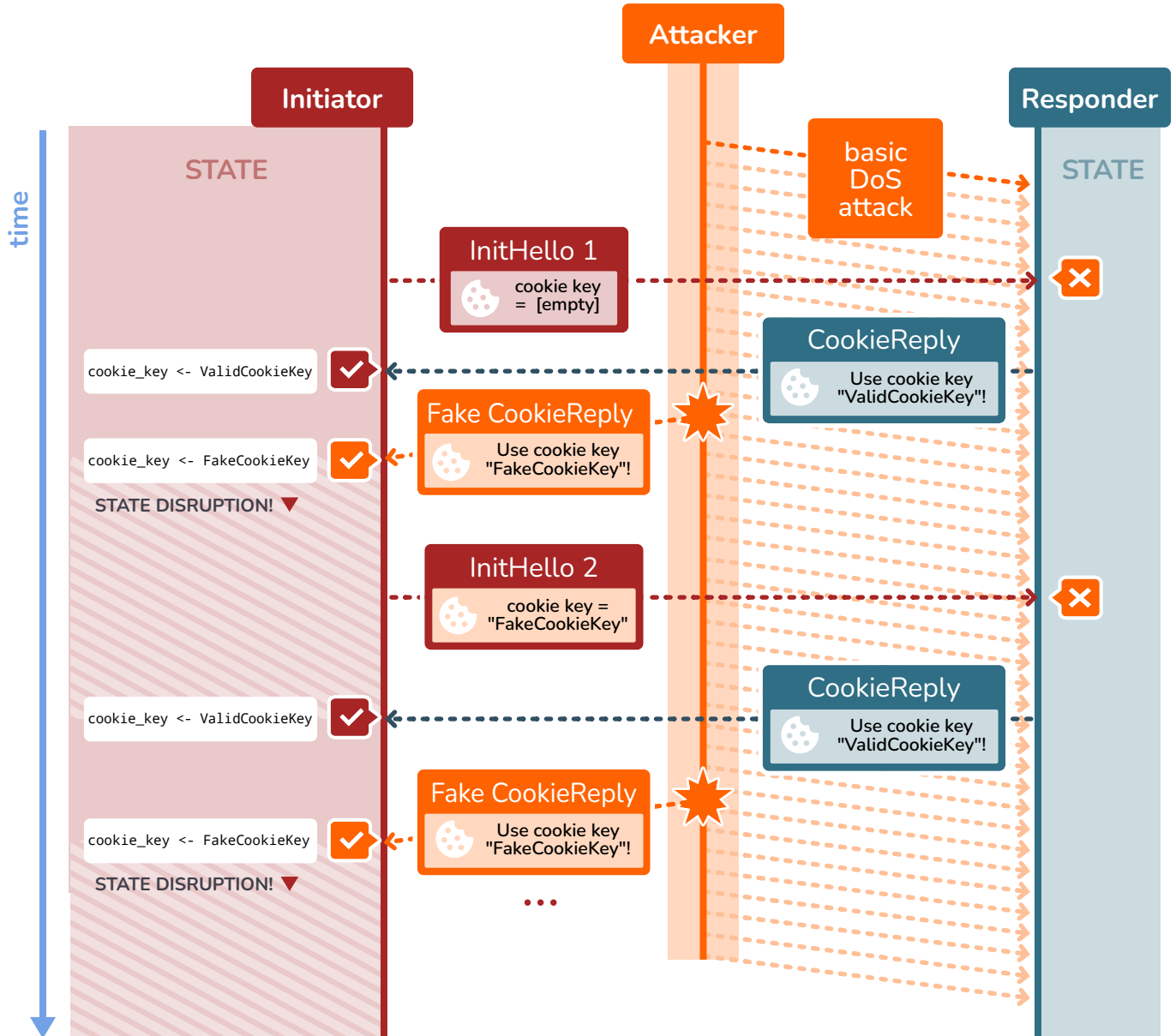
# Post-Quantum WireGuard allows state disruption since InitHello is unauthenticated



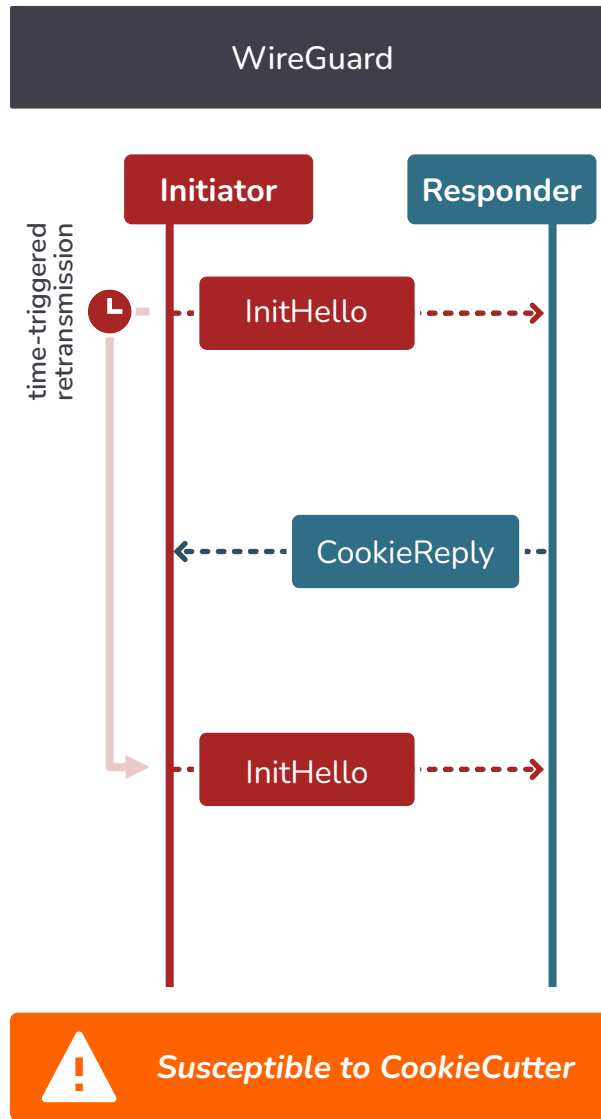


# CookieCutter attack against WireGuard

state disruption attack against WireGuard based on the "Proof of IP ownership" cookie mechanism

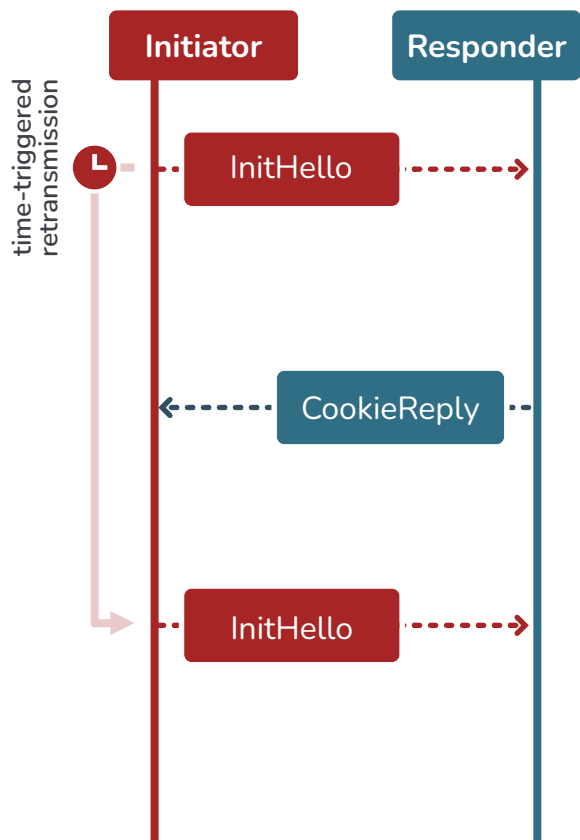


## CookieCutter Susceptibility – WireGuard



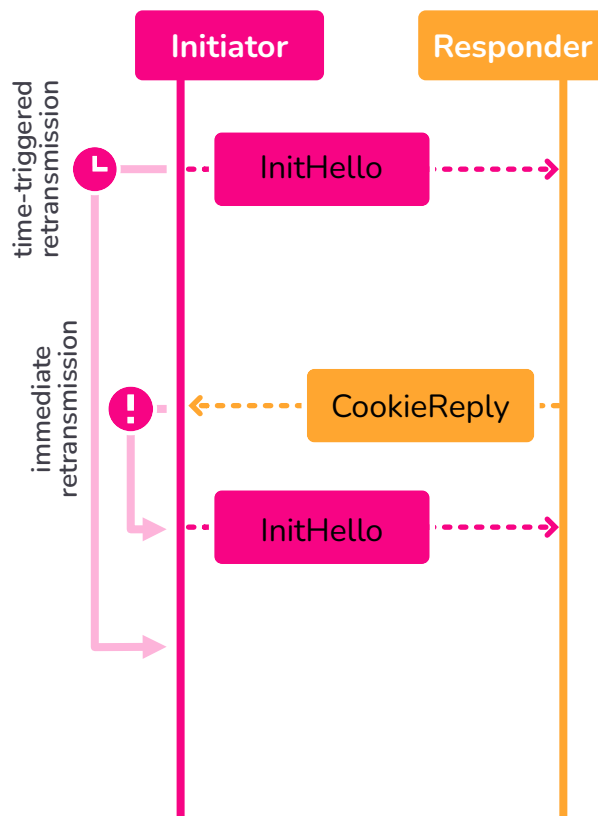
# CookieCutter Susceptibility – WireGuard vs Rosenpass

## WireGuard



*Susceptible to CookieCutter*

## Rosenpass



*Not susceptible due to immediate retransmission upon CookieReply*

InitHello and CookieReply must be of same size to avoid amplification DoS attacks