

Distance-Bounding Protocols

CHARLIE WANG, JINGCHI ZHANG
APRIL 9, 2018

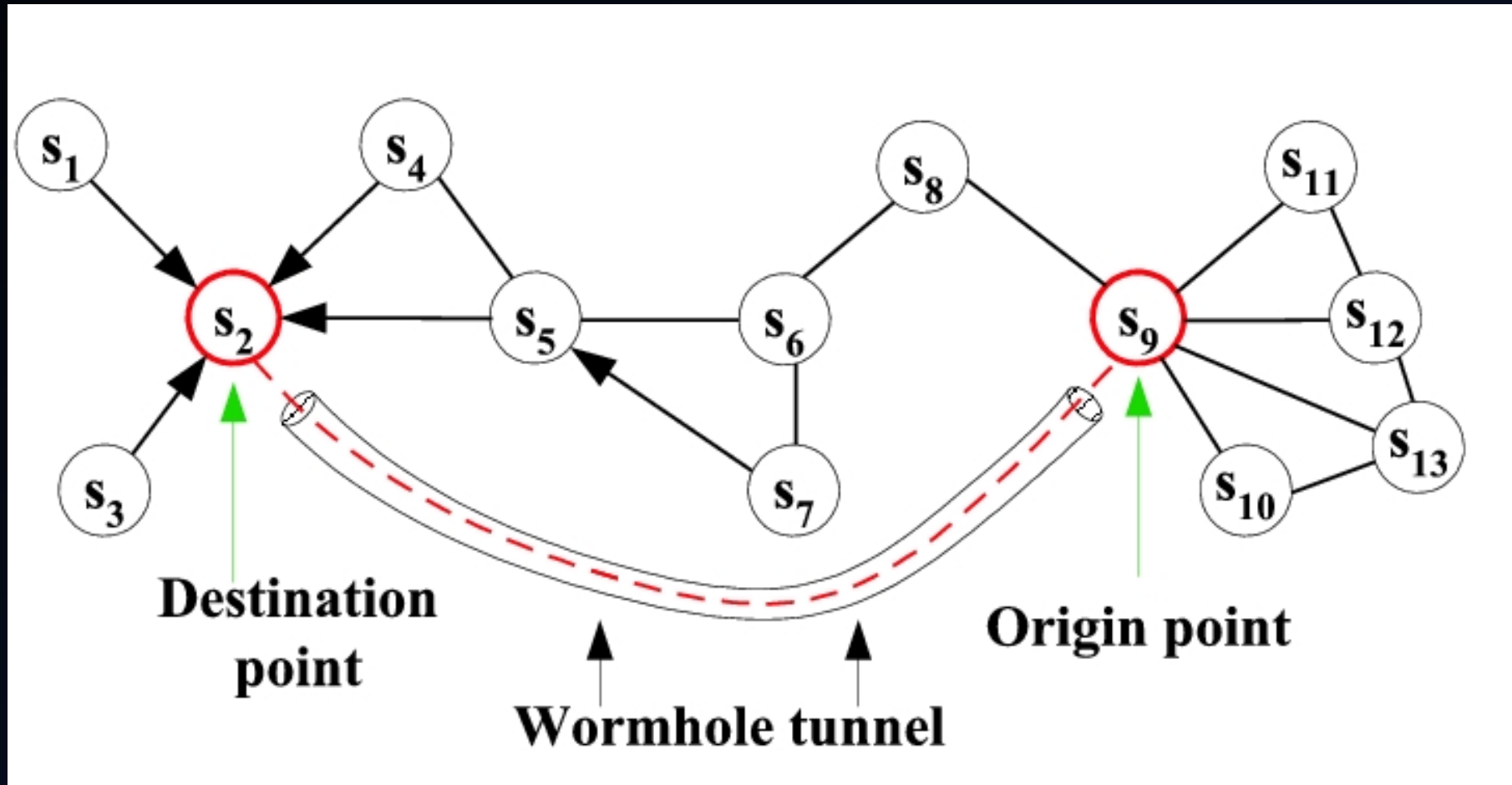
ADVANCED TOPICS IN APPLIED CRYPTOGRAPHY
EN.600.745, JOHNS HOPKINS UNIVERSITY

Motivation

Passive Keyless Entry Systems



Wormholes



Contactless Systems



RFID

NFC

Leads to a new notion

Distance-Bounding Protocol

The slide features a dark blue background. On the left side, there are several parallel teal lines that form a corner-like shape. On the bottom right, there are several parallel teal lines that extend diagonally across the corner.

But let's start with

Protocol Basics

Basics of Protocols

- A protocol is the interaction between 2 or more agents
 - Agents = computer or process. Able to carry out some action
 - Each agent has a Role = specified behavior of the agent
- A security protocol is a protocol that runs within an untrusted environment and aims to achieve a security goal

The 3 Protocol Agents

- **Prover:** aims to show it is at most d distance away
 - Can be Honest or Dishonest
- **Verifier:** wants to know that P is at most d away
 - Assumed to be Honest
- **Adversary (Intruder):** wants to cheat the protocol
 - Can construct new messages, eavesdrop, delay, block, forge, inject. And can recruit new adversaries

P

V

A

Standard protocol interaction

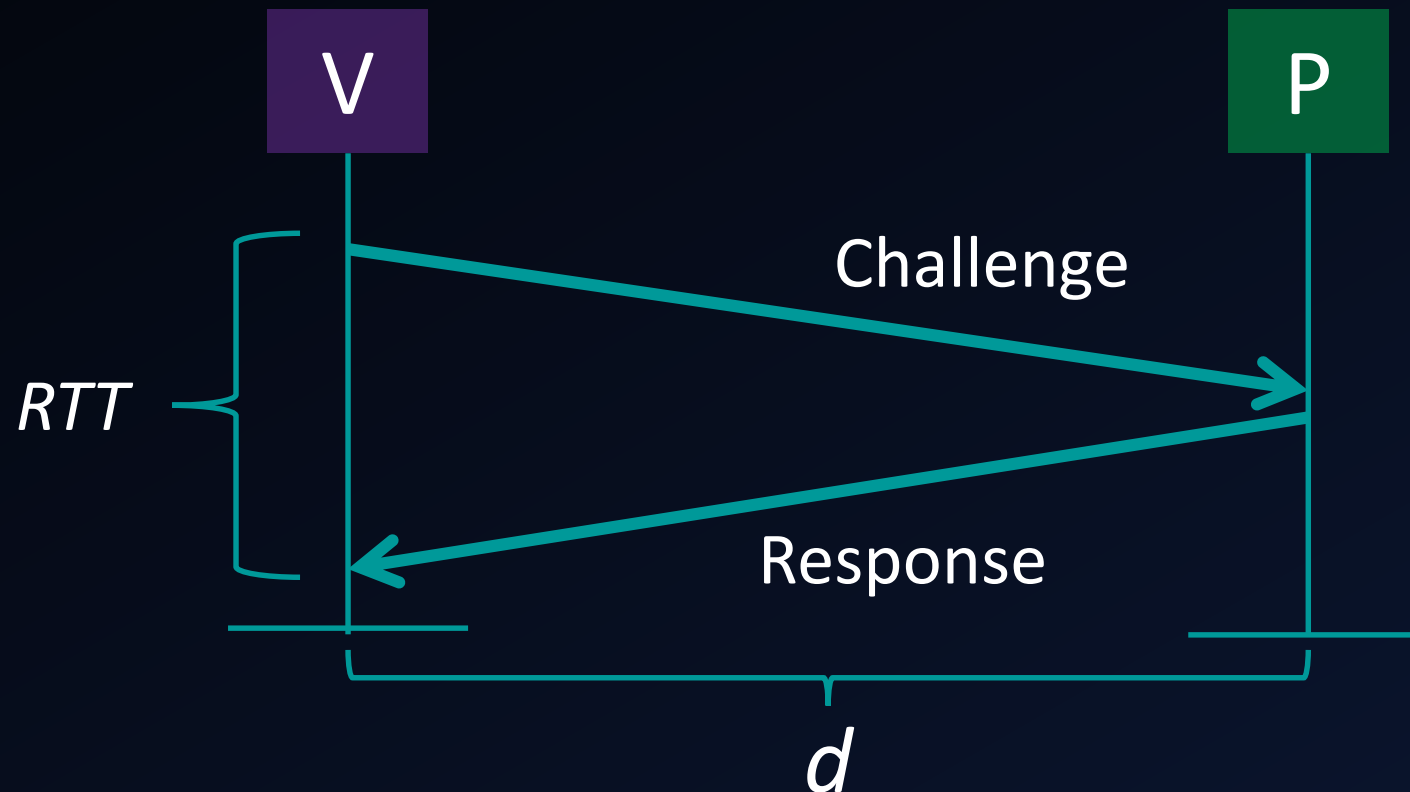


Now adding

Distance-Bounding

What is a distance-bounding protocol

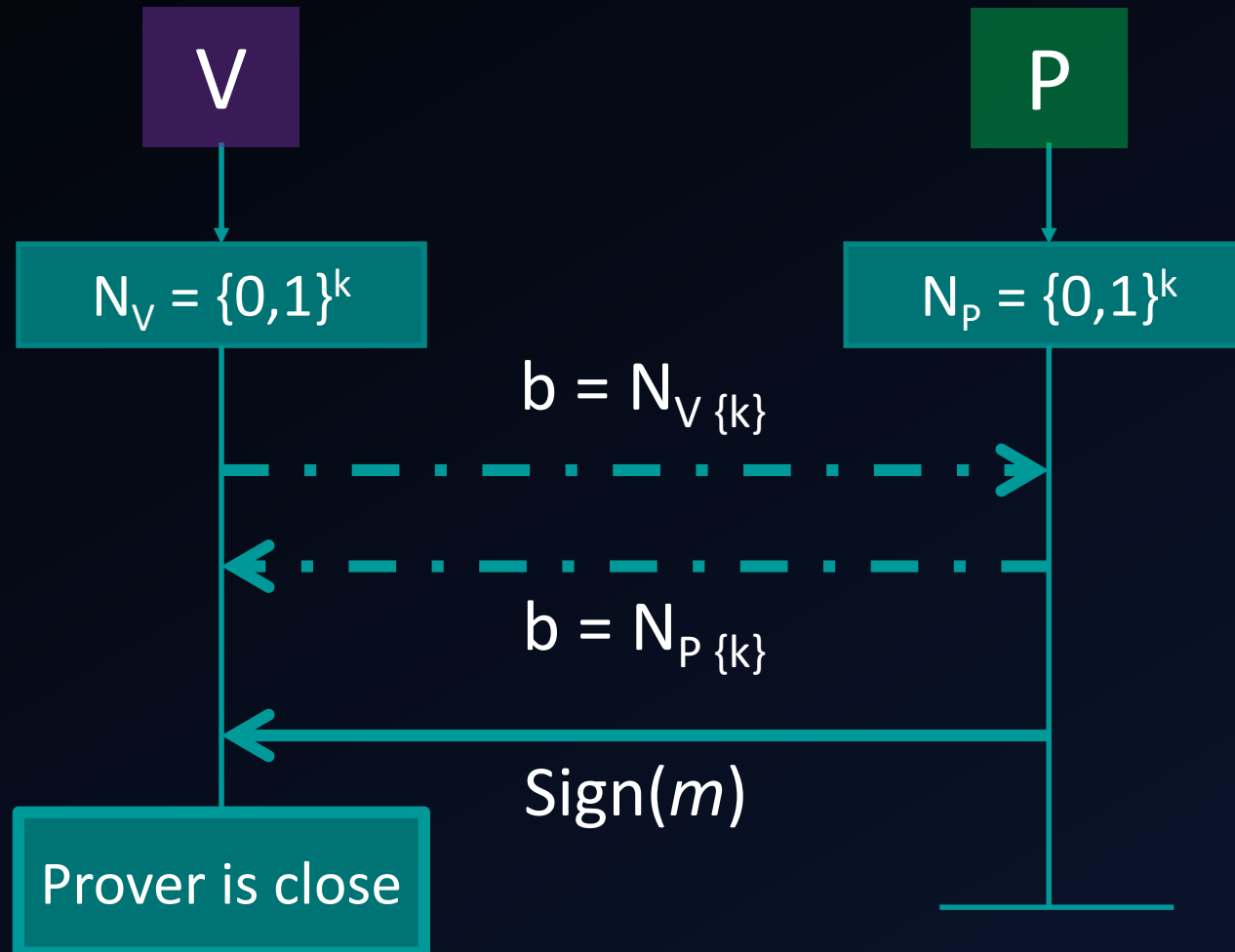
- Purpose: prove to the Verifier that the Prover is physically located not more than a specified distance d away



The essence of distance-bounding

1. Use 1+ challenge/response rounds
2. Measure the Round-Trip Time = RTT
3. Indirectly obtain upper bound on distance
 - Prover-to-Verifier distance = d
 - Speed of light = c
 - Upper bound: $d \leq (RTT/2) * c$

Brands and Chaum (1993)



Slow Phase

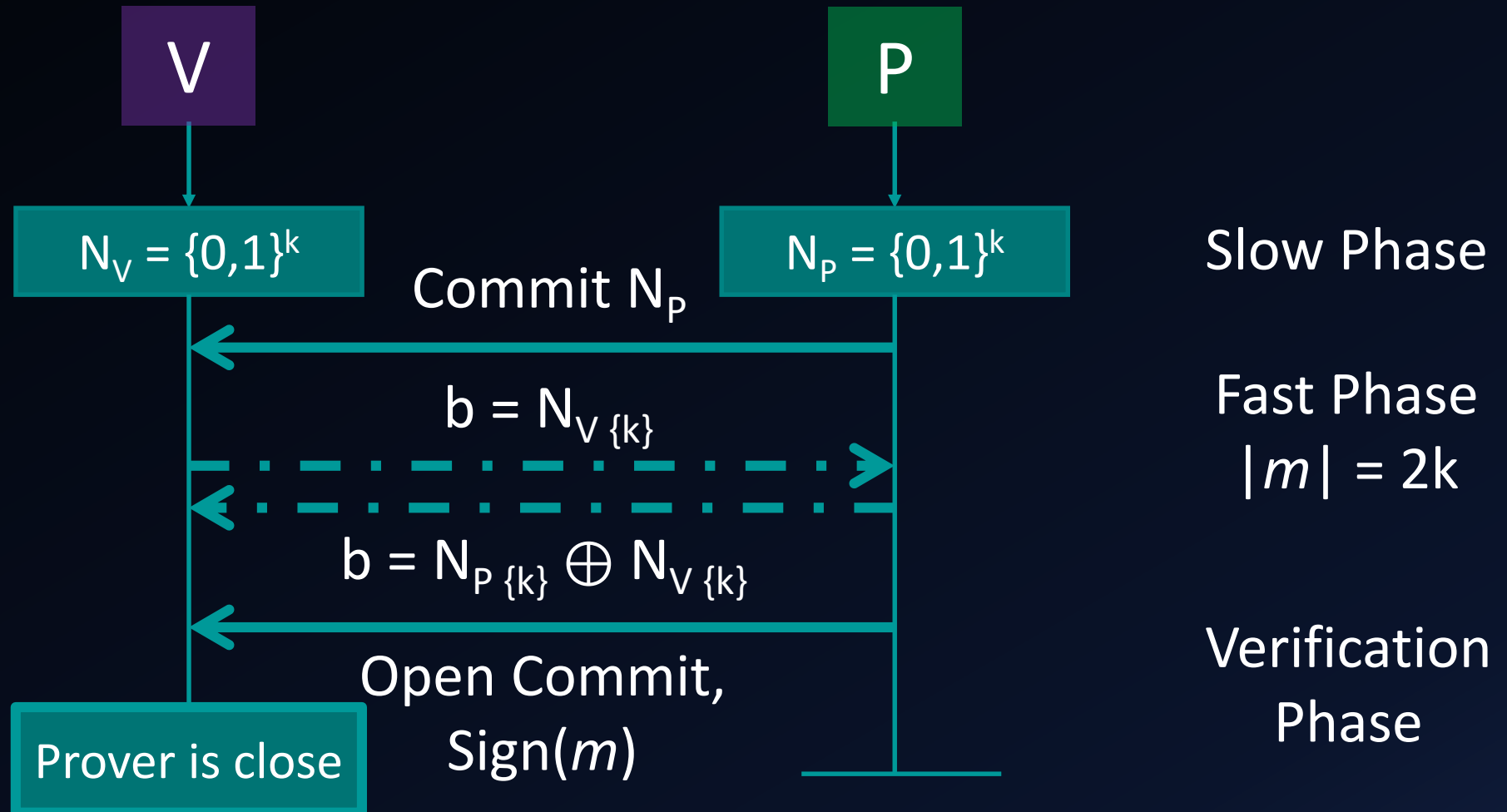
Fast Phase
 $|m| = 2k$

Verification
Phase

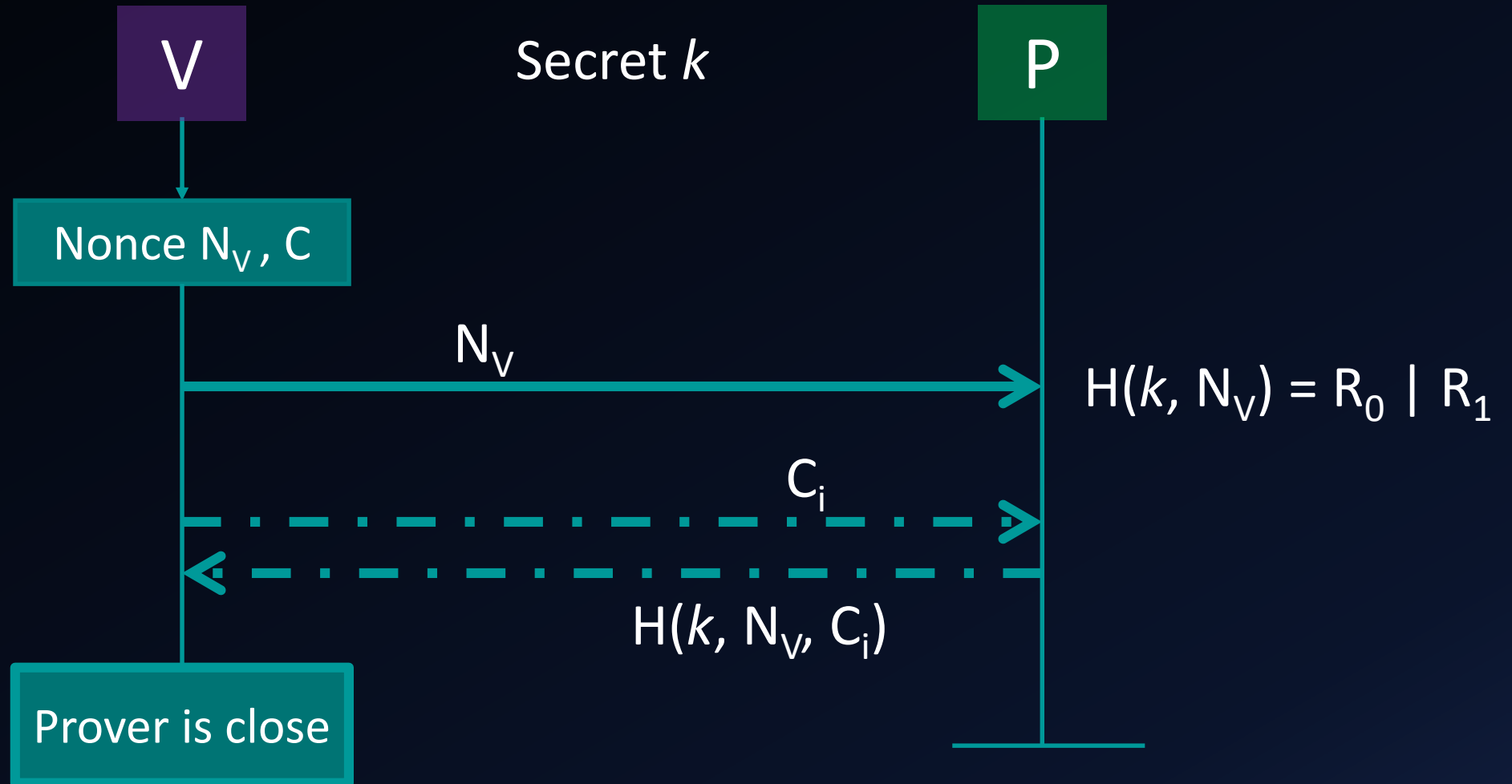
Attack on Brands and Chaum

- Nothing is preventing the prover from sending bits sooner than receiving the bits from the verifier.
- The prover can pretend to be closer than it really is.
- How do we fix this?

Brands and Chaum: Final Construction



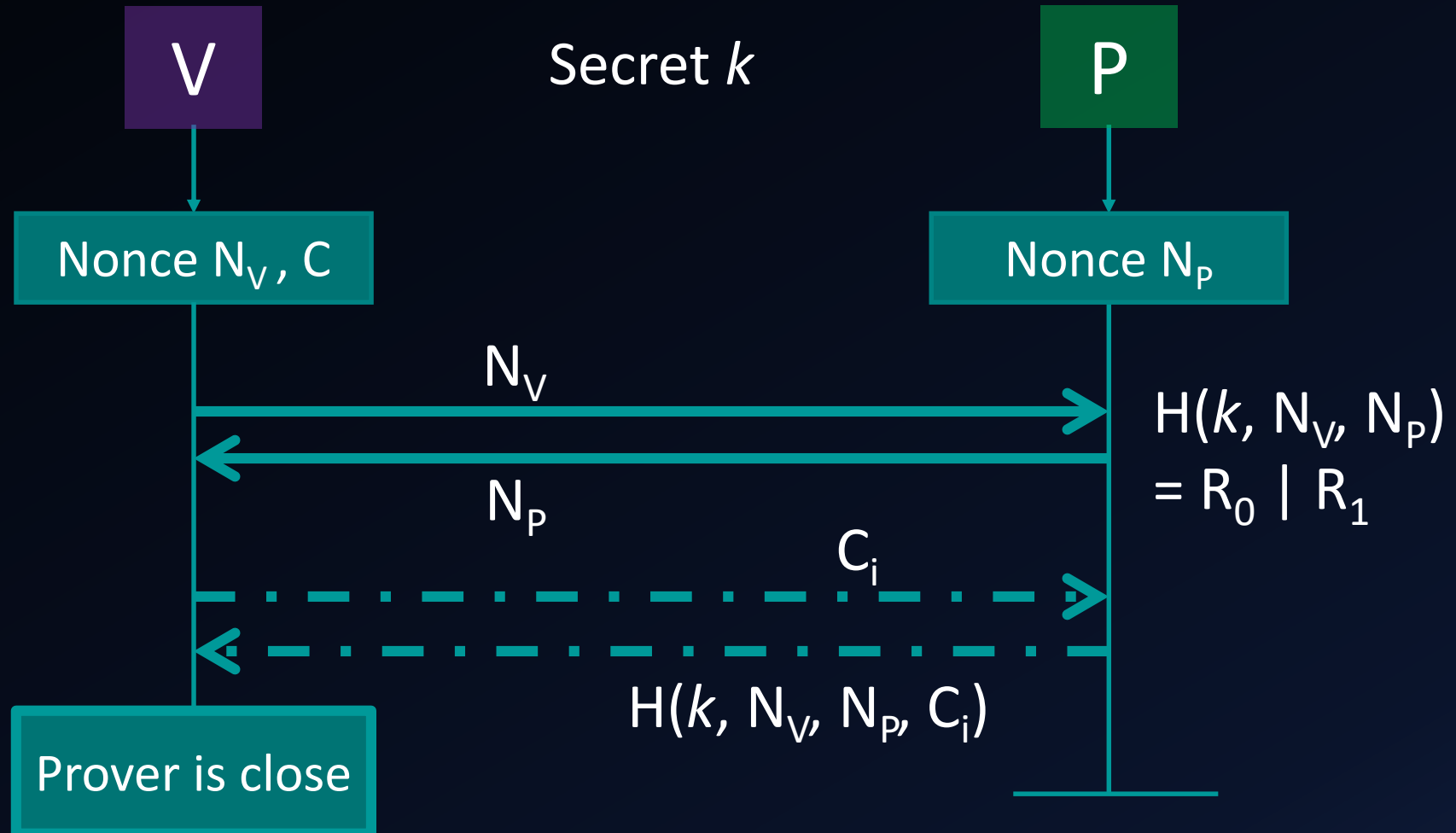
Hancke and Kuhn (2005)

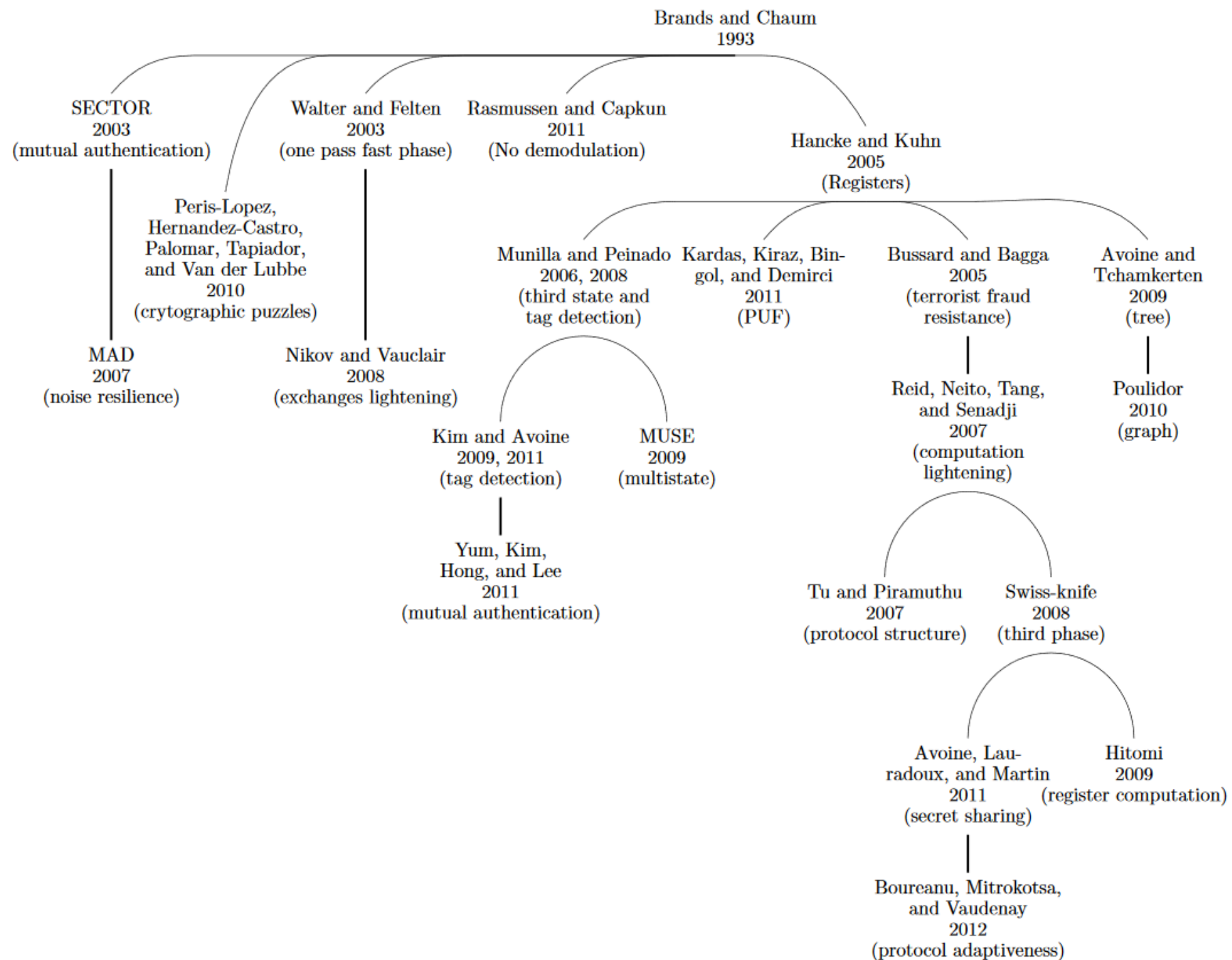


An attack on Hancke and Kuhn

1. Adversary runs the protocol 2x with Prover using the same nonce in both runs
2. Adversary recovers the entire $H(k, N_v) = R_0 \mid R_1$
3. Adversary then can act as a **dishonest prover** by running the protocol with the Verifier

Hancke and Kuhn: Final Construction





Traditionally, a well-designed protocol is resistant to 3 types of attacks

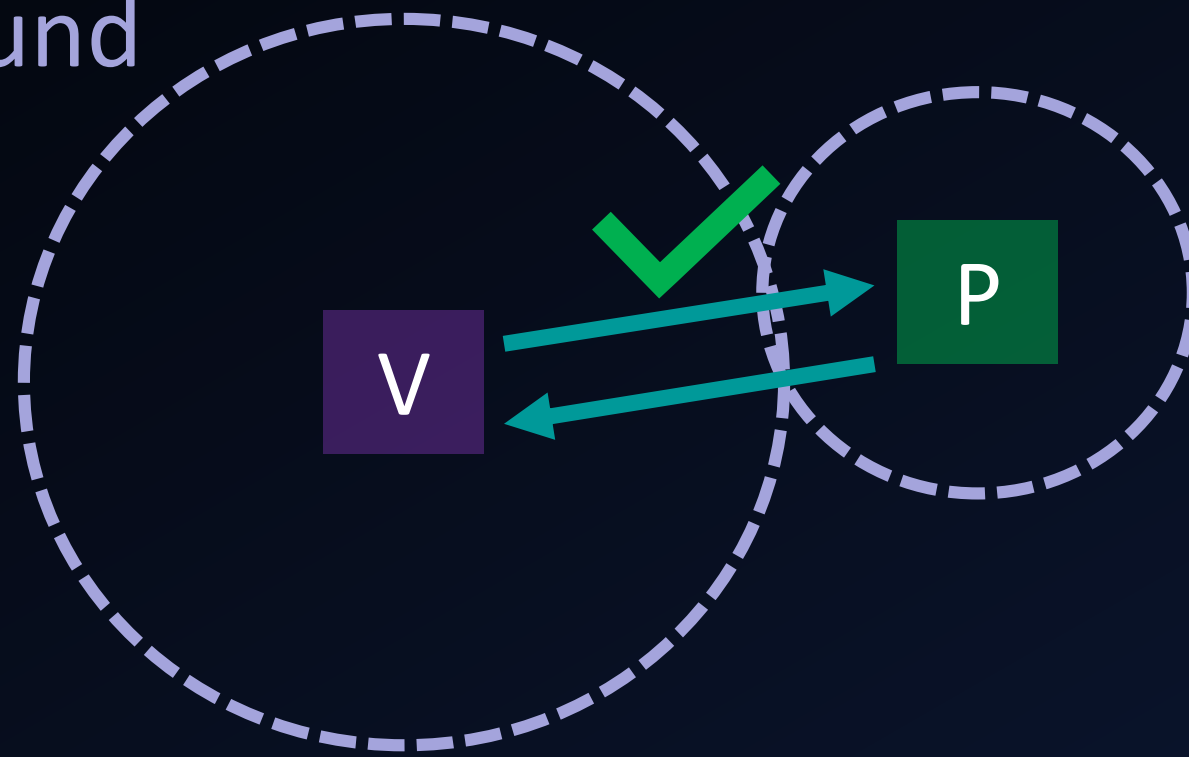
Mafia
Fraud

Terrorist
Fraud

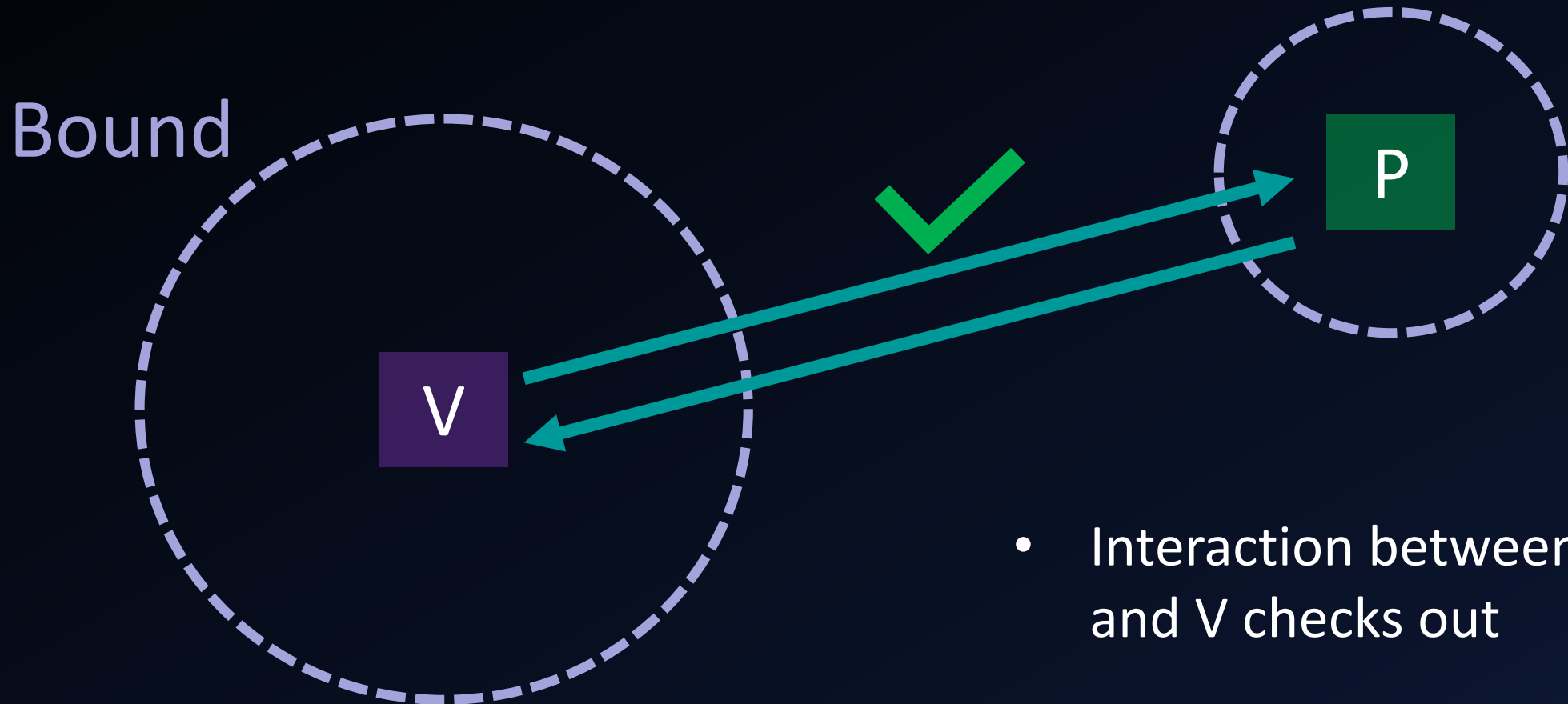
Distance
Fraud

Supposedly

Bound

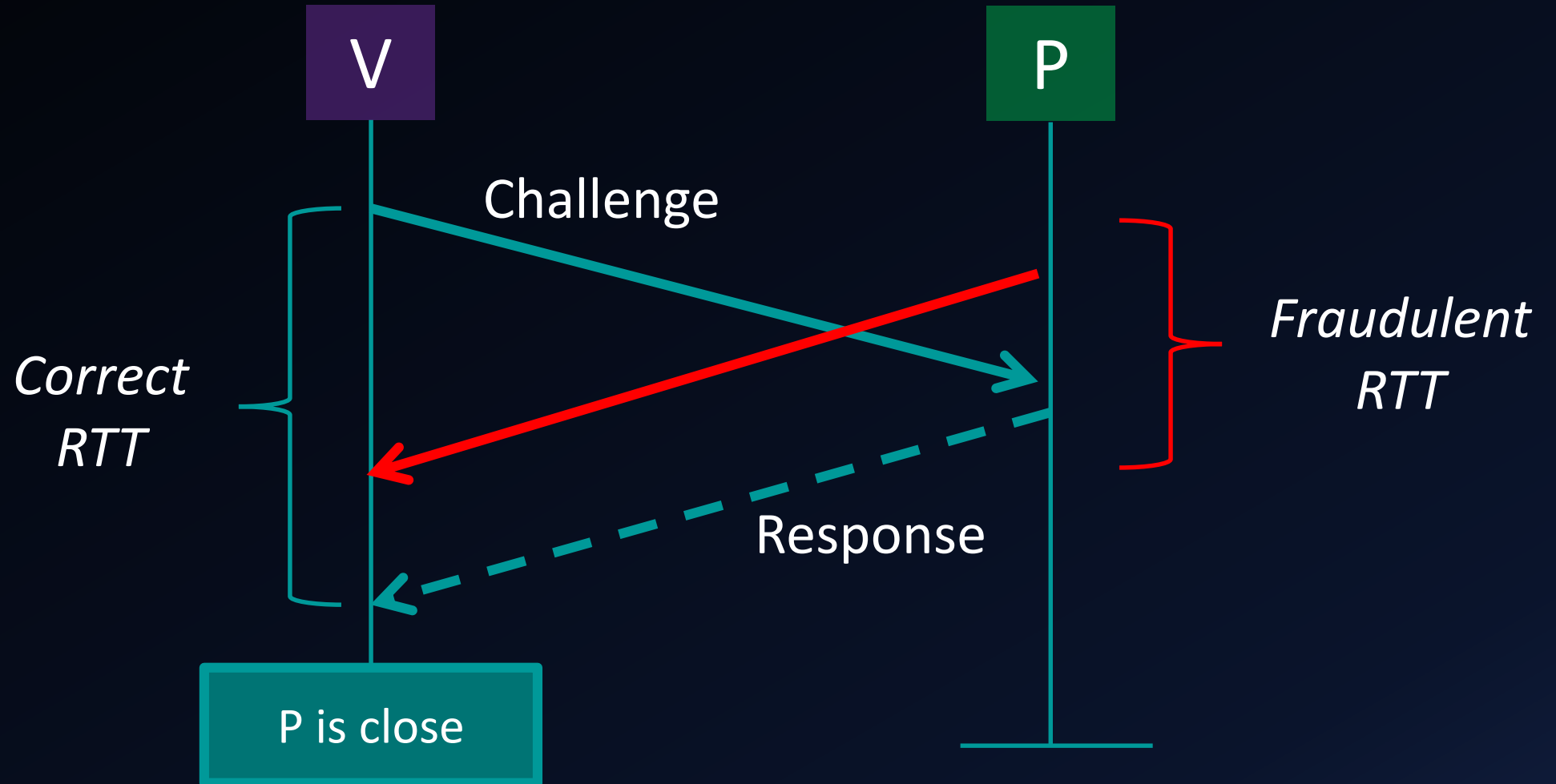


Motivation behind Distance Fraud

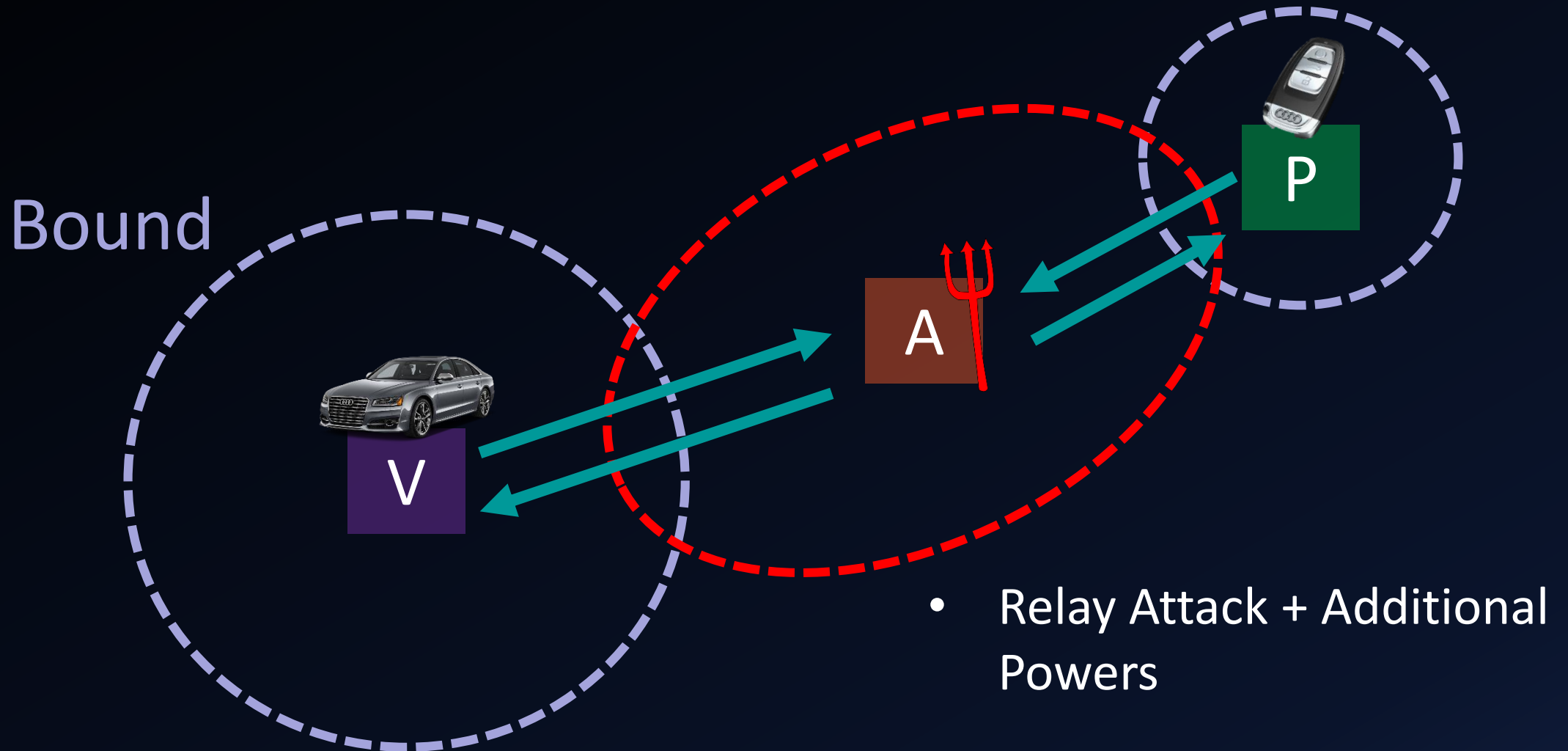


- Interaction between P and V checks out

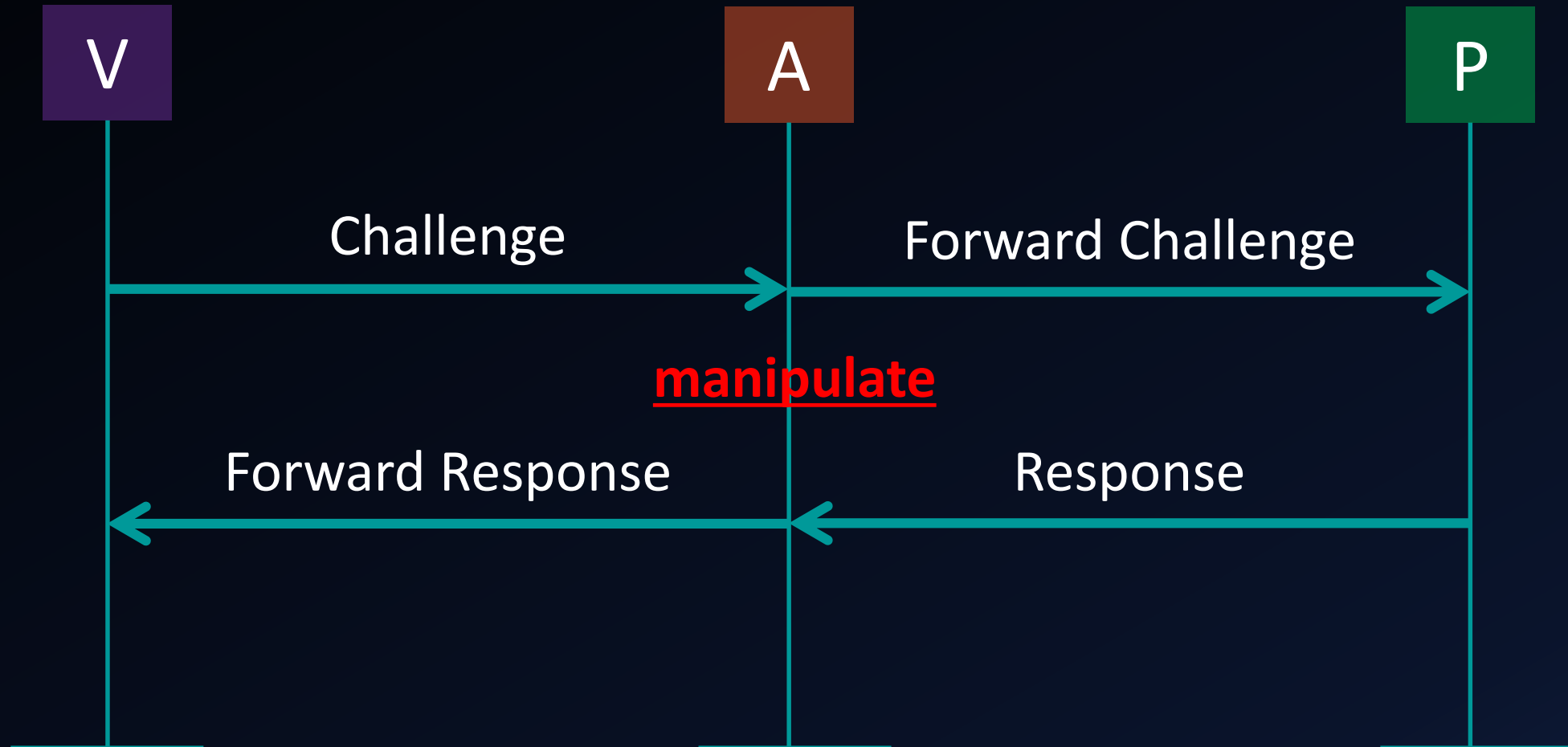
Distance Fraud within a protocol



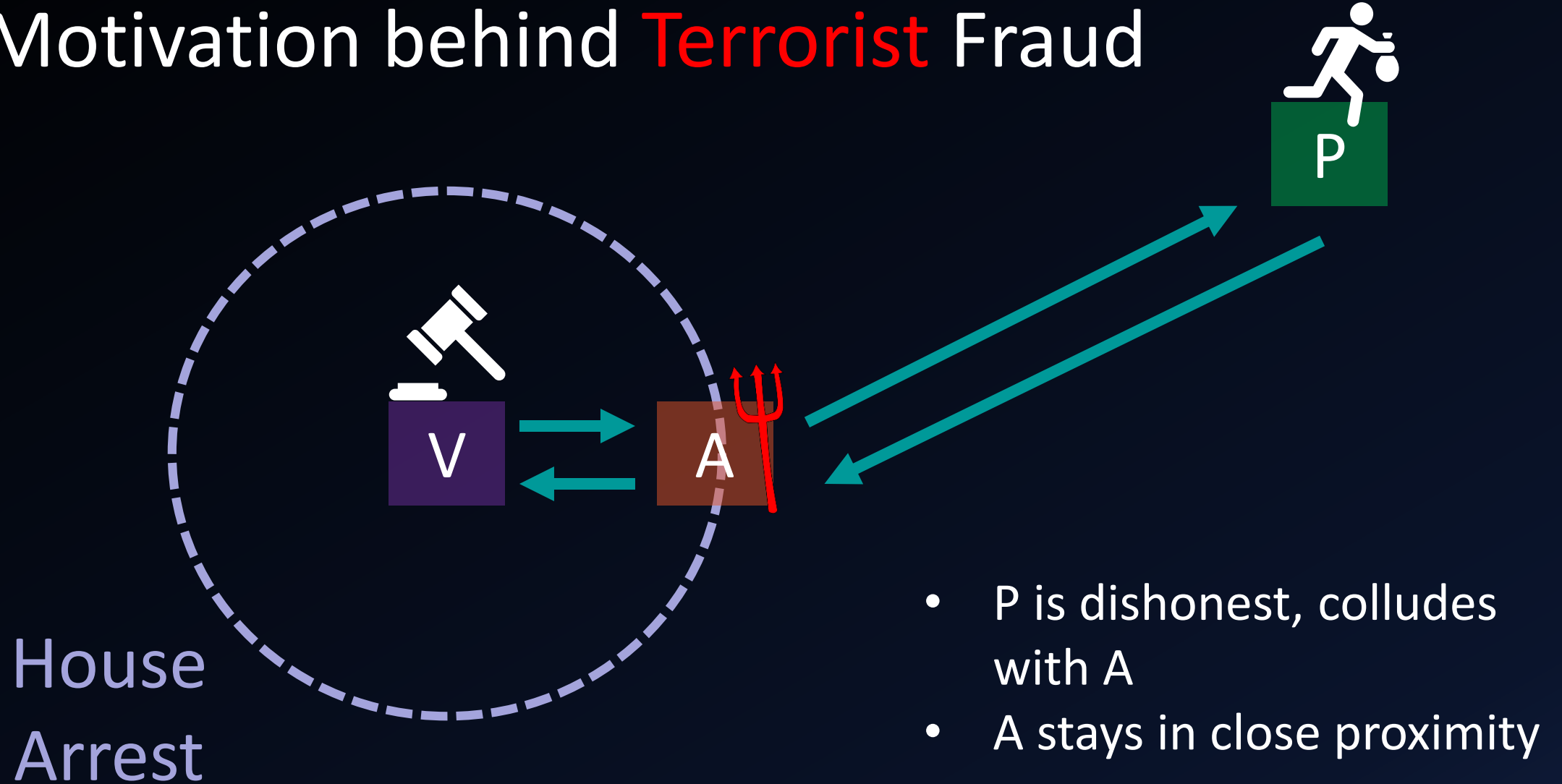
Motivation behind Mafia Fraud



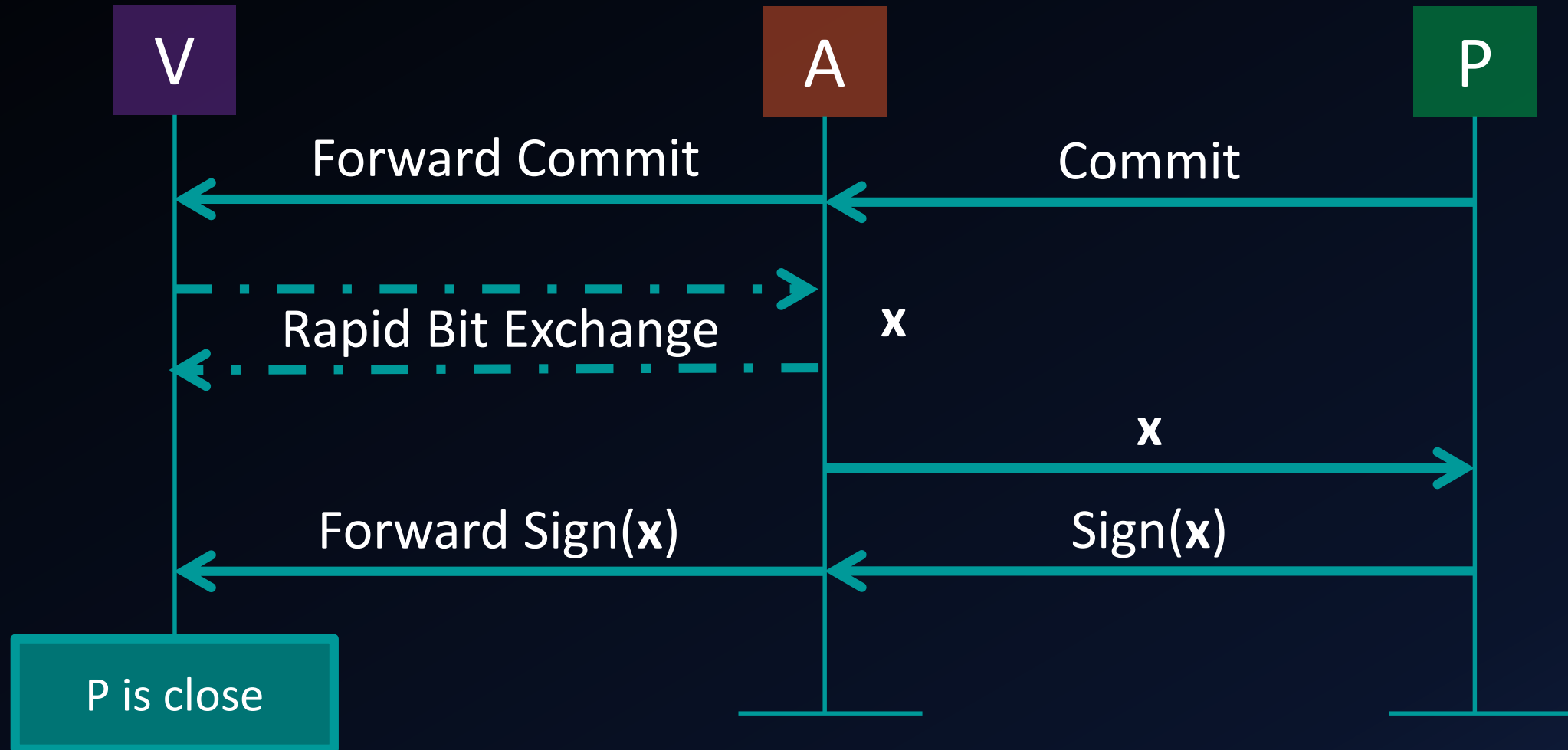
Mafia Fraud within a protocol



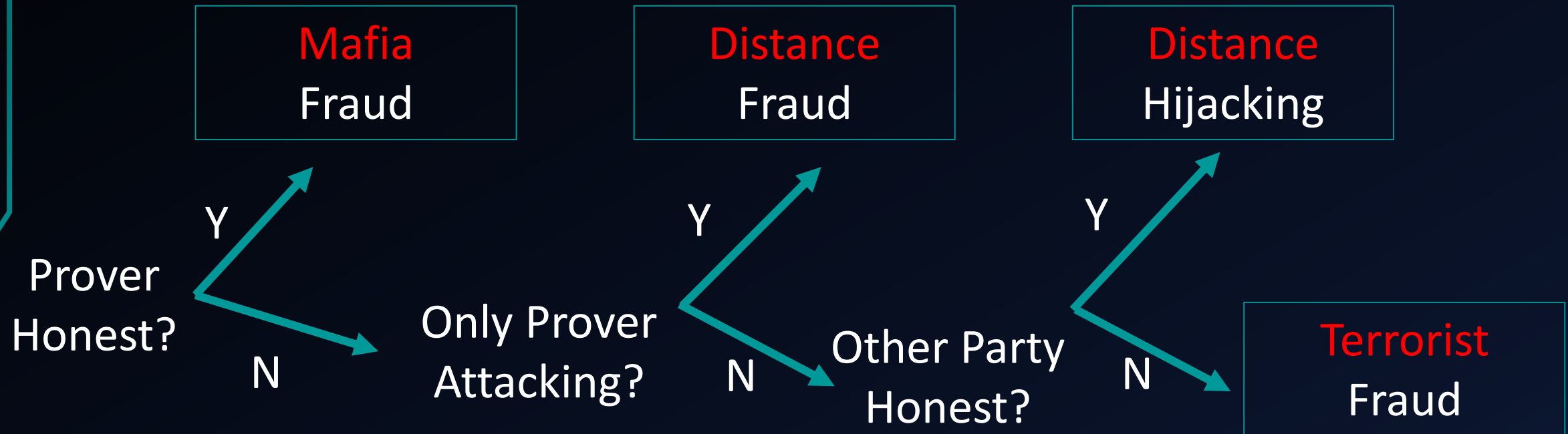
Motivation behind Terrorist Fraud



Terrorist Fraud within a protocol



Flow of classifying the attack



And there are more attacks

Overshadowing

...

Distance
Hijacking

Symbolic and Computational Model

Security Analysis

SYMBOLIC MODEL

- Developed by Needham and Schroeder, and Dolev and Yao
- Often called Dolev-Yao model

COMPUTATIONAL MODEL

- Developed by Goldwasser, Micali, Rivest, Yao, and others

Computational model

- Manual proofs of security properties in an ad-hoc proof model.
- Proof models are often game based.
- Proofs are done by reduction to known hard problems (e.g. discrete log, factorization).

Symbolic model

- Find attacks by exhibiting all possible behavior (traces) of a protocol.
- Can be combined with other techniques for correctness proofs.
- $\text{dec}(\text{enc}(x,y),y) = x$

Security Analysis

SYMBOLIC MODEL

- Suitable for automation
- Compute the set of all messages the adversary can know

COMPUTATIONAL MODEL


- More realistic
- But complicates the proof,
- Proof only manual

Security analysis for Distance-Bounding Protocols

- Symbolic or Computational?
- Not straightforward and complex VS high user intervention
- Well-established automated verification tools (Tamarin, ProVerif and Scyther)

What if

- time and location are indeed not needed to specify and verify the security of distance-bounding protocols



Let's Formalize

Time and Location protocol

Protocol Grammar

1. $\text{Msg} ::= \text{atom} \mid (\text{Msg}, \text{Msg}) \mid \{\text{Msg}\}\text{Msg} \mid f(\text{Msg})$
2. $\text{Ev} ::= \text{sendA}(\text{Msg})[\text{Msg}] \mid \text{recvA}(\text{Msg}) \mid \text{claimA}(\text{B}, \text{Ev}, \text{Ev})$
3. $\text{init}(\text{A}) = \text{Agent A} \cup \text{Const} \cup \text{NonceA}$
 $\quad \cup \{\text{sk}(\text{A})\}$
 $\quad \cup \{\text{pk}(\text{B}) \mid \text{B} \in \text{Agent}\}$
 $\quad \cup \{\text{sh}(\text{A}, \text{B}) \mid \text{B} \in \text{Agent}\}$

Protocol Variables

1. A trace α is a finite sequence of timed-events $\alpha \in (R \times Ev)^*$, representing the execution of a protocol.
2. $dmA(\alpha)$ denotes the set of all deducible messages from a trace α
3. For a given protocol P , the set of possible traces $Tr(P)$ defined by the Start rule (Start), the Intruder rule (Int), the Network rule (Net) and the rules specifying the protocol
4. $max_t(\alpha) = \max_{(t,e) \in \alpha} \{t\}$, yields the latest time at which an event of α occurred

Network Rules

$$\frac{}{\epsilon \in \text{Tr}(\mathcal{P})} \text{ Start}$$

$$\frac{\alpha \in \text{Tr}(\mathcal{P}) \quad I \in \text{Dishonest} \quad t \geq \text{maxt}(\alpha) \quad m \in \text{dm}_I(\alpha)}{\alpha \cdot (t, \text{send}_I(m) []) \in \text{Tr}(\mathcal{P})} \text{ Int}$$

$$\frac{\alpha \in \text{Tr}(\mathcal{P}) \quad t \geq \text{maxt}(\alpha) \quad (t', \text{send}_A(m) [s]) \in \alpha \quad t \geq t' + d(A, B) / c}{\alpha \cdot (t, \text{recv}_B(m)) \in \text{Tr}(\mathcal{P})} \text{ Net}$$

Protocol Specification

1. Behavior of dishonest agents is fully specified by the intruder rule
2. Agents are unaware of what other agents do

Protocol Properties

- Agents are unaware of what other agents do.
- The model uses claim events as placeholders to indicate where a security property needs to be satisfied
- $\text{claim}_v(P, u, v)$

Protocol Definition

- A protocol P satisfies **secure distance-bounding** if and only if:

$\forall \alpha \in \text{Tr}(P), V, P \in \text{Agent}, u, v, w \in \text{Ev}, t_w \in \mathbb{R}:$

$(t_w, w) \in \alpha \wedge w = \text{claim}_V(P, u, v) \Rightarrow$

$\exists t_u, t_v \in \mathbb{R}, P' \in \text{actor}(\alpha) :$

$(t_u, u) \in \alpha \wedge (t_v, v) \in \alpha \wedge P \approx P' \wedge d(V, P') \leq (c/2) (t_v - t_u)$

Basic Protocol Properties

1. A protocol P satisfies **time consistency** if for every trace $\alpha = (t_1, e_1) \cdots (t_n, e_n) \in \text{Tr}(P)$, it holds that $t_1 \leq \cdots \leq t_n$.
2. A protocol P satisfies **speed-of-light consistency** if for every trace $\alpha = (t_1, e_1) \cdots (t_n, e_n) \in \text{Tr}(P)$ the following holds: for all $j \in \{2, \dots, n\}$, if $e_j \in \text{Recv}$, then there exists $i \in \{1, \dots, j-1\}$ such that $e_i \rightarrow e_j$ and $t_j - t_i \geq d(e_i, e_j)/c$.

Basic Protocol Properties

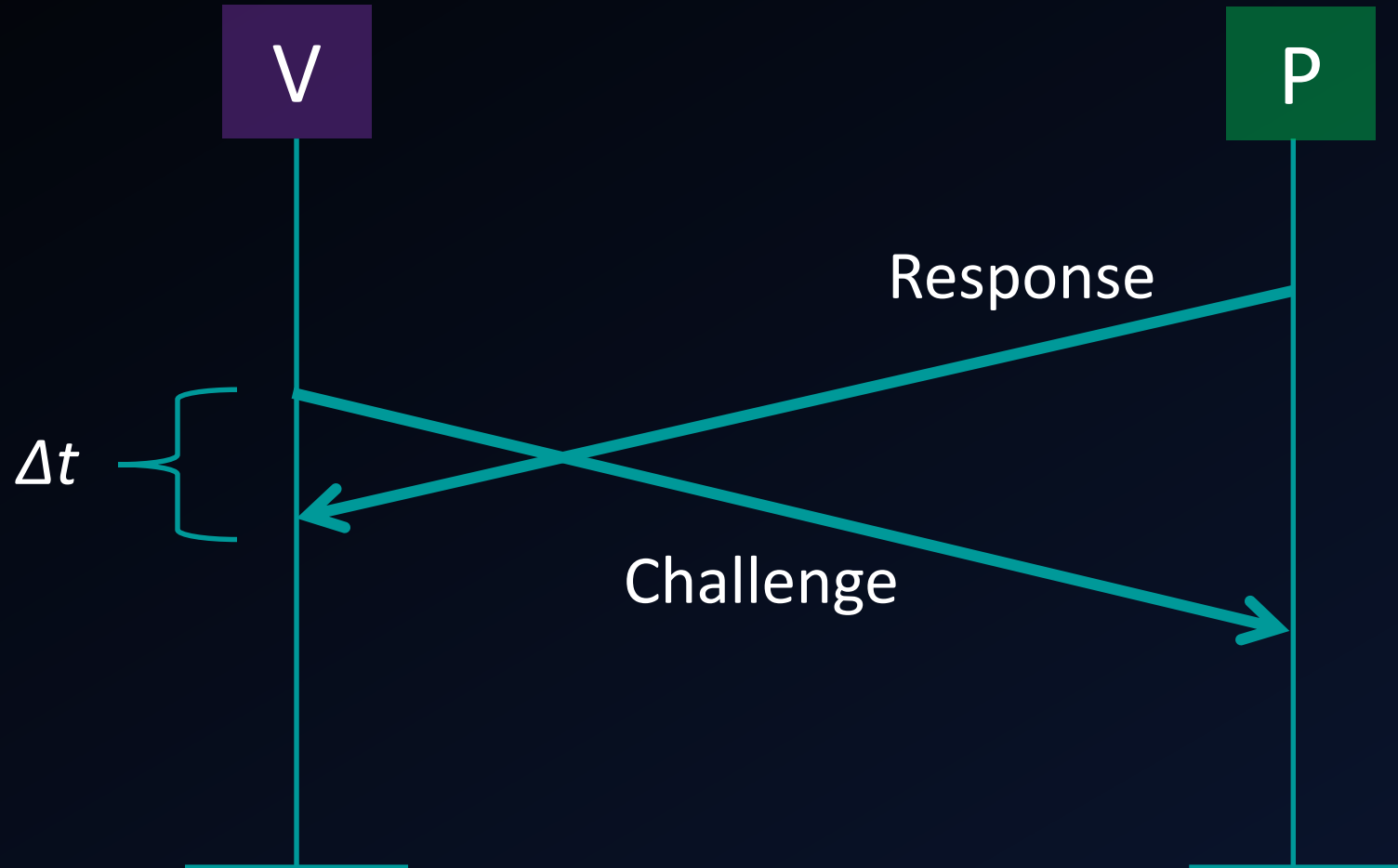
3. A protocol P is **prefix-closed** if for every $\gamma = \sigma \cdot e \in \pi(\text{Tr}(P))$, it holds that $\sigma \in \pi(\text{Tr}(P))$.
4. A protocol P is **time-unaware** if for every trace $\alpha \in \text{Tr}(P)$ the following holds: for all time consistent and speed-of-light consistent traces $\beta \in (R \times \text{Ev})^*$, $\alpha \sim \beta$ implies $\beta \in \text{Tr}(P)$.
5. A protocol P satisfies **locally-enabled events** if for every $\gamma = \sigma \cdot e \cdot e' \in \pi(\text{Tr}(P))$ such that $e' \notin \text{Recv}$ and $\text{actor}(e) \neq \text{actor}(e')$, it holds that $\sigma \cdot e' \in \pi(\text{Tr}(P))$.

Basic Protocol Properties

6. A protocol P satisfies **transmission-enabled events** if for every $\gamma = \sigma \cdot e \in \pi(\text{Tr}(P))$ and every $e' \in \text{Recv}$ such that $e \rightarrow e'$, it holds that $\gamma \cdot e' \in \pi(\text{Tr}(P))$.
7. A protocol P is **substitution-closed** if for every $\sigma \in \pi(\text{Tr}(P))$ and every $A, B \in \text{Agent}$ such that $\{A, B\} \subseteq \text{Honest}$ or $\{A, B\} \subseteq \text{Dishonest}$, it holds that $\sigma[A \mid \rightarrow B] \in \pi(\text{Tr}(P))$.

New distance-bounding Causality-Based protocol

Intuition: causality based on ordering



Causality-Based formal definition

- A well-formed protocol P satisfies **causality-based secure distance-bounding** if and only if:

$\forall \sigma \in \pi(\text{Tr}(P)), \quad \forall V, P \in \text{Agent}, \quad u, v \in \text{Ev}:$

$\text{claim}_V(P, u, v) \in \sigma \Rightarrow$

$\exists i, j, k \in \{1, \dots, |\sigma|\}:$

$i < j < k \wedge u = \sigma_i \wedge v = \sigma_k \wedge P \approx \text{actor}(\sigma_j)$



Questions?

Lemma 1

- Let P be a well-formed protocol. Then the following holds:

$\forall \alpha \in \text{Tr}(P), (t,e) \in R \times \text{Ev}: \alpha \cdot (t,e) \in \text{Tr}(P) \Rightarrow$

$\exists \beta \in \text{Tr}(P) : (t,e) \in \beta \wedge \beta \text{ is a subsequence of } \alpha \cdot (t,e)$

$\wedge \psi(\beta)$

Lemma 2

- Let P be a well-formed protocol and $\alpha \in \text{Tr}(P)$ such that $\psi(\alpha)$. Then

$\forall (t, e), (t', e') \in \alpha$ it holds that

$$|t - t'| \geq d(e, e')/c$$

Proof of Lemma 2

Use the triangle inequality

$$d(e,e')/c + d(e',e'')/c \geq d(e,e'')/c, \text{ for all } e,e',e'' \in E_v$$

Let $\alpha = (t_1, e_1) \cdots (t_n, e_n)$ and $i, j \in \{1, \dots, n\}$. Assume without loss of generality that $i < j$. Given that $\psi(\alpha)$ we have that $t_x - t_{x-1} \geq d(e_{x-1}, e_x)/c$ for all $x \in \{i+1, \dots, j\}$. Hence

$$t_j - t_i = (t_j - t_{j-1}) + (t_{j-1} - t_{j-2}) + \cdots + (t_{i+1} - t_i) \geq d(e_i, e_{i+1})/c + d(e_{i+1}, e_{i+2})/c + \cdots + d(e_{j-1}, e_j)/c.$$

Apply triangle inequality to get $t_j - t_i \geq d(e_i, e_j)/c$

Lemma 3

- Let P be a well-formed protocol and $\alpha = (t_1, e_1) \cdots (t_n, e_n) \in \text{Tr}(P)$. Let $A \in \text{actor}(\alpha)$, $B \in \text{Agent} \setminus \text{actor}(\alpha)$ such that either $\{A, B\} \subseteq \text{Honest}$ or $\{A, B\} \subseteq \text{Dishonest}$.

Then there exists $\mu \in R_{\geq 0}$ such that $\alpha' = (t_1', e_1') \cdots (t_n', e_n') \in \text{Tr}(P)$ where for all $i \in \{1, \dots, n\}$ it holds that:

$e_i' = e_i [A \mid \rightarrow B]$ and $t_i' = t_i + \mu \cdot q_i$, where

$q_i = |\{j \in \{1, \dots, i-1\} \mid \text{actor}(e_j) = A\}| + s_i$, and

$s_i = 1$ if $(A = \text{actor}(e_i) \wedge e_i \in \text{Recv})$, or otherwise $s_i = 0$

Proof of Lemma 3

Consider the set $R = \{B\} \cup \text{actor}(\alpha)$ and $\mu = \max \text{ of } d(A, X)/c$ where $X \in R$. Need to prove that $\alpha' \in \text{Tr}(P)$.

In order to do so, need to prove

1. Time Consistency
2. Speed-of-light Consistency

Proof of Time Consistency

For all $i \in \{1, \dots, n-1\}$, have

$q_{i+1} \geq q_i$ and therefore

$$t'_{i+1} - t'_i = t_{i+1} - t_i + \mu \cdot (q_{i+1} - q_i) \geq t_{i+1} - t_i \geq 0$$

Proof of Speed of Light Consistency

Let $j \in \{1, \dots, n\}$ such that $e_j \in \text{Recv}$.

Also, as α is speed-of-light consistent, we derive that there exists $i < j$ such that $e_i \rightarrow e_j$ and $t_j - t_i \geq d(e_i, e_j)/c$.

Hence, given that $e_{i'} \rightarrow e_{j'}$, it becomes sufficient to prove that $t_{j'} - t_{i'} \geq d(e_{i'}, e_{j'}) / c$.

Now consider 3 cases.

Proof of Speed of Light Consistency cont..

- 1) $A = \text{actor}(e_i)$. In this case $q_j \geq q_i + 1$ because $e_i \notin \text{Recv}$.
Therefore $t_j' - t_i' \geq t_j - t_i + \mu \geq d(e_i', e_j')/c$ as $\mu \geq d(e_i', e_j')/c$
- 2) $A \neq \text{actor}(e_i)$ and $A = \text{actor}(e_j)$. In this case we have again $q_j \geq q_i + 1$ as $e_j \in \text{Recv}$, and it follows analogously to the previous case.
- 3) $A \notin \{\text{actor}(e_i), \text{actor}(e_j)\}$. This case gives us $\text{actor}(e_i) = \text{actor}(e_0)$ and $\text{actor}(e_j) = \text{actor}(e_j)$. Thus, $d(e_i, e_j)/c = d(e_i', e_j')/c$ and therefore $t_j' - t_i' = t_j - t_i + \mu \cdot (q_j - q_i) \geq t_j - t_i \geq d(e_i, e_j)/c = d(e_0, e_j)/c$

Proof of Lemma 3 cont...

Thus, α' is time consistent and speed-of-light consistent.

Consider now $\sigma = \pi(\alpha)$. From Substitution-Closed Property, we have that $\sigma[A \mid \rightarrow B] \in \pi(\text{Tr}(P))$.

Therefore, there exists $\gamma \in \text{Tr}(P)$ such that $\pi(\gamma) = \sigma[A \mid \rightarrow B]$.

Finally, given that $\gamma \sim \alpha'$, from Time-Aware Property ($\alpha \sim \beta$ implies $\beta \in \text{Tr}(P)$), $\alpha' \in \text{Tr}(P)$.