Key Consistency and Discovery

`draft-wood-key-consistency`

Davidson, Finkel, Thomson, Wood — IETF 114 — Privacy Pass

Motivation
Background

Emerging privacy-focused protocols require a mechanism for clients to discover server public keys

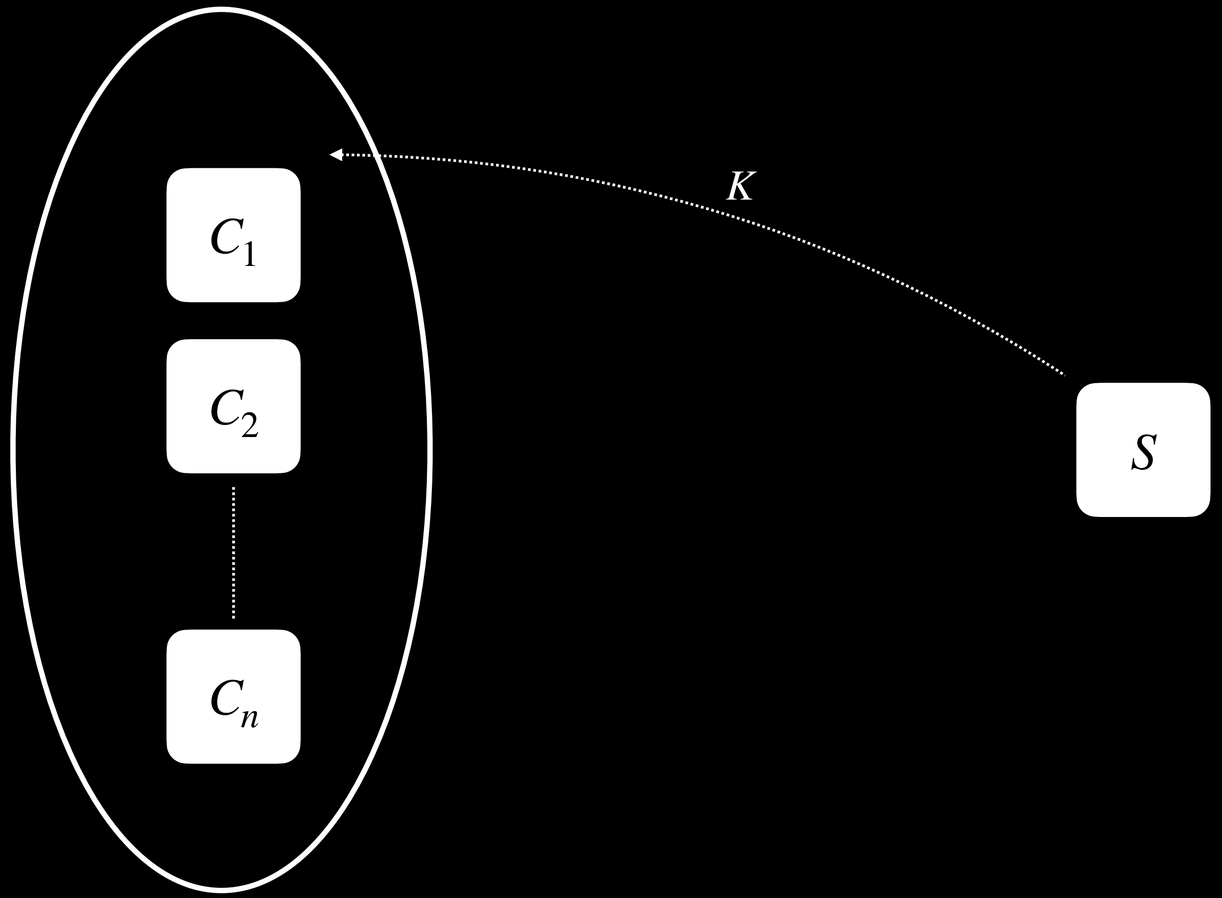
- Privacy Pass: Issuer verification key
- OHTTP: Gateway public encryption key
- Tor: Relay public keys

Common requirements:

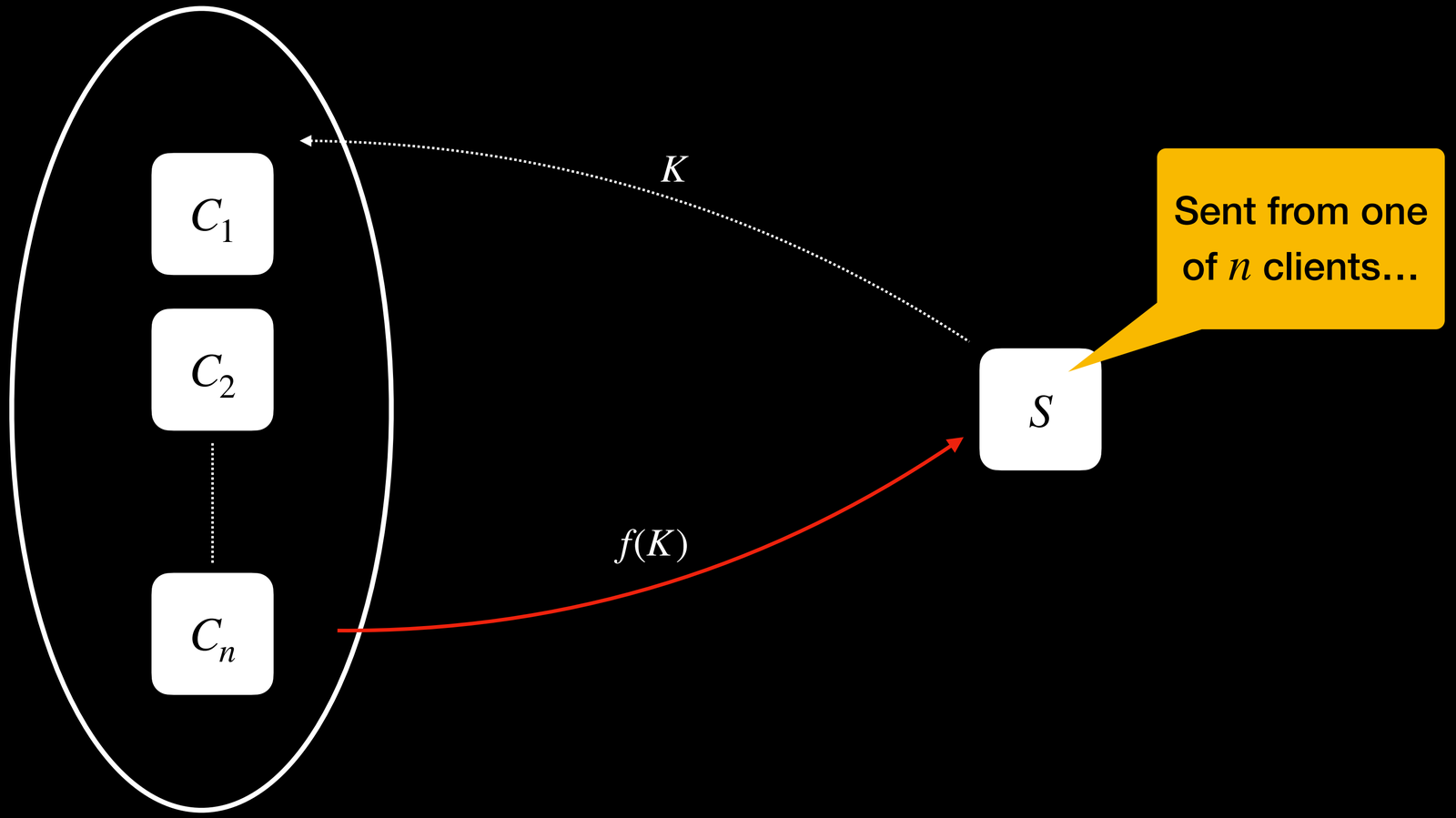
1. Unlinkability: Servers cannot *link usage of a key to specific users*
2. Authenticity: Clients use an *authentic* key for the intended server

Motivation

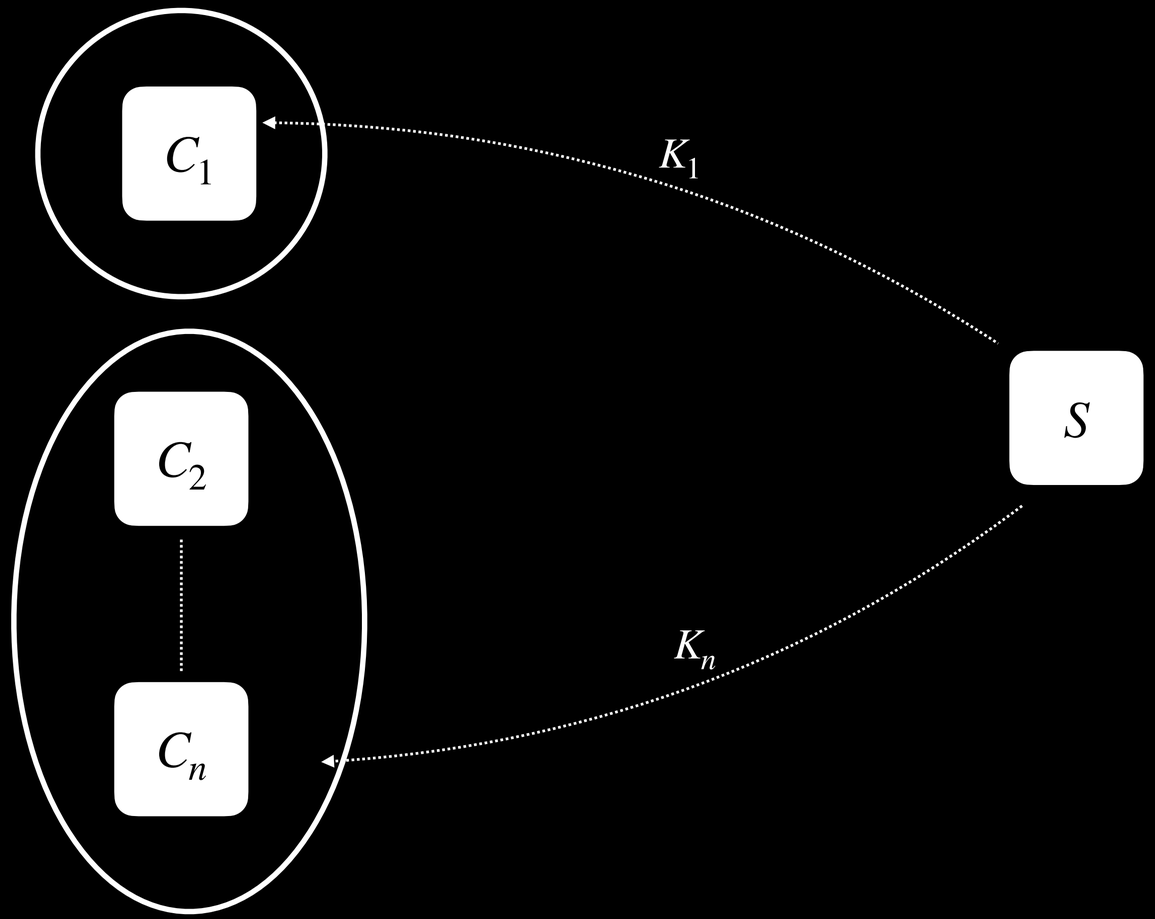
Unlinkability



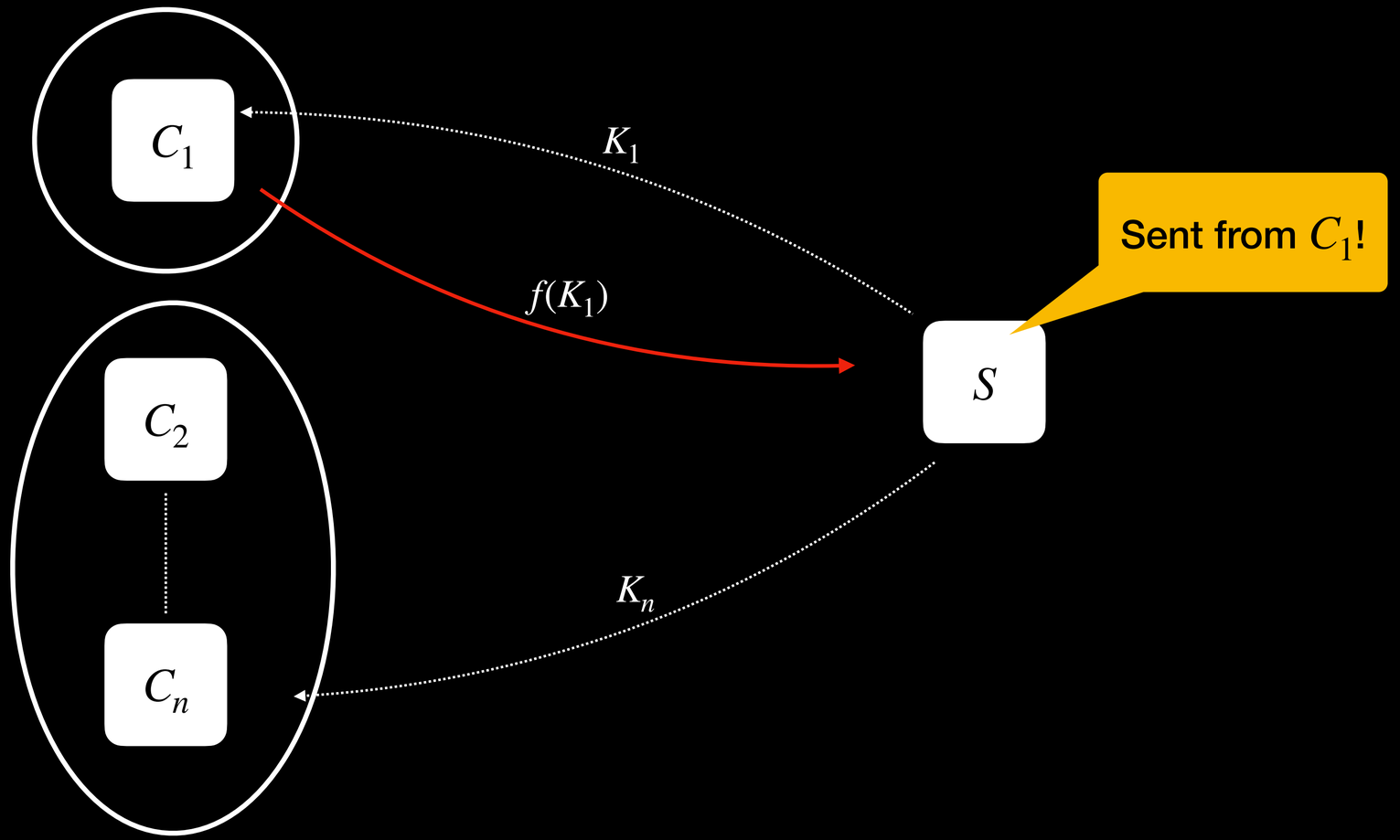
Motivation
Unlinkability



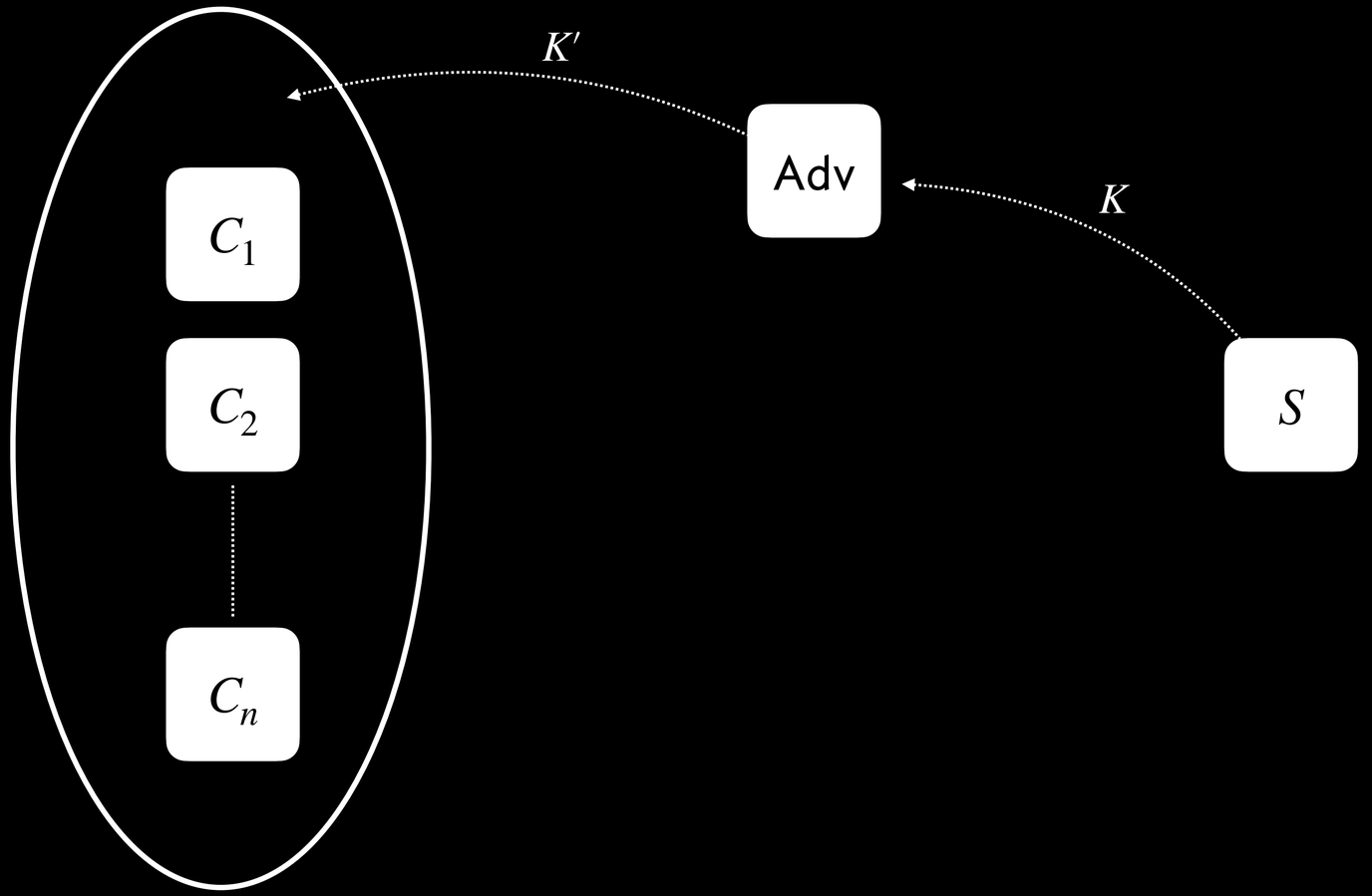
Motivation
Unlinkability



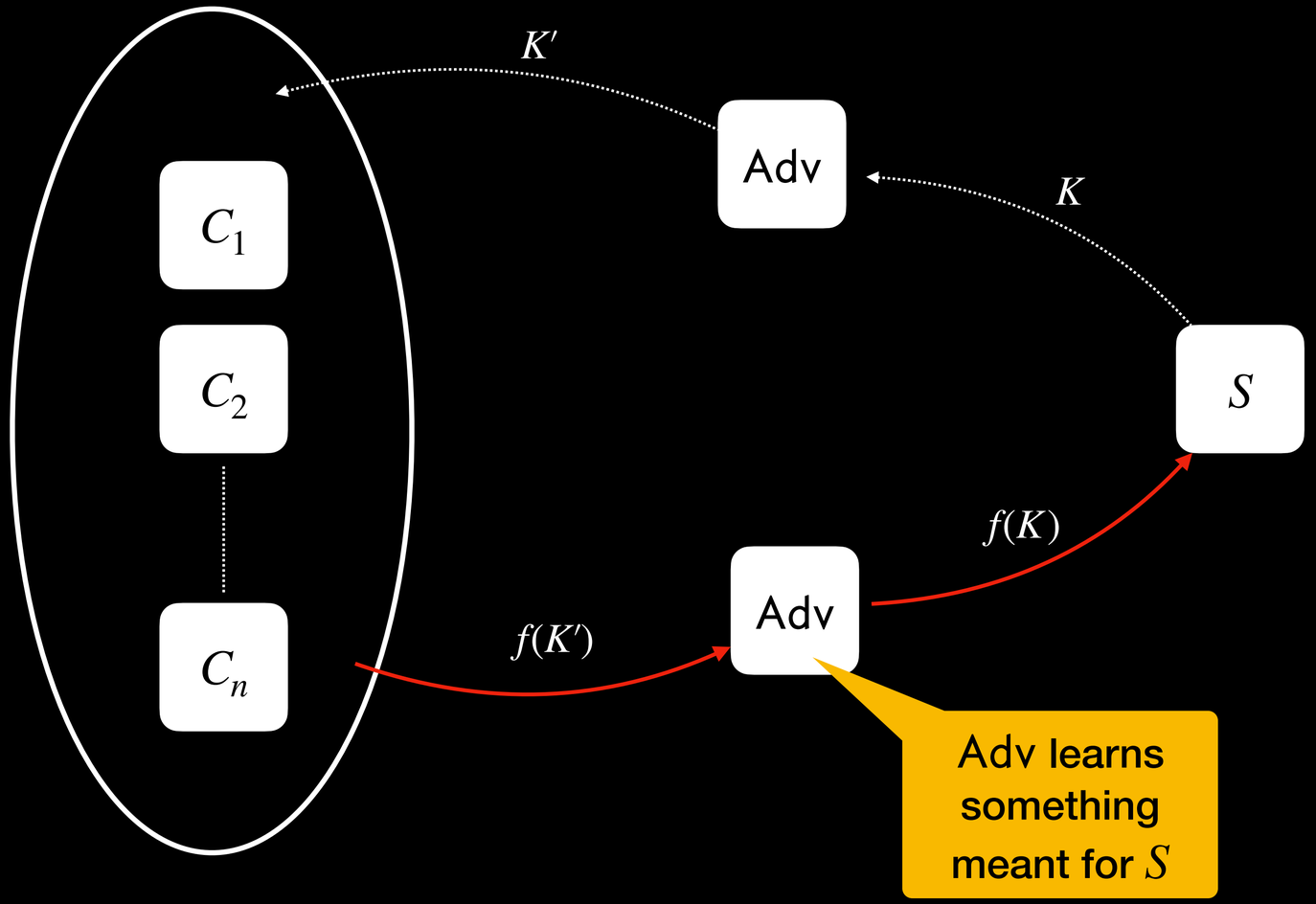
Motivation
Unlinkability



Motivation
Authenticity



Motivation
Authenticity



Unlinkability and authenticity means that all clients in the same anonymity set have a ***consistent*** view of the server's intended key, and that view is ***correct***

Consistency and Correctness

In practice

A key consistency and correctness system (KCCS) is something that provides consistency and correctness for clients

KCCS varies in practice based on:

- Threat model
- Cryptographic dependencies
- Trust model and PKI
- Operational complexity
- External dependencies

Consistency and Correctness

Design space

Fetch through a trusted proxy

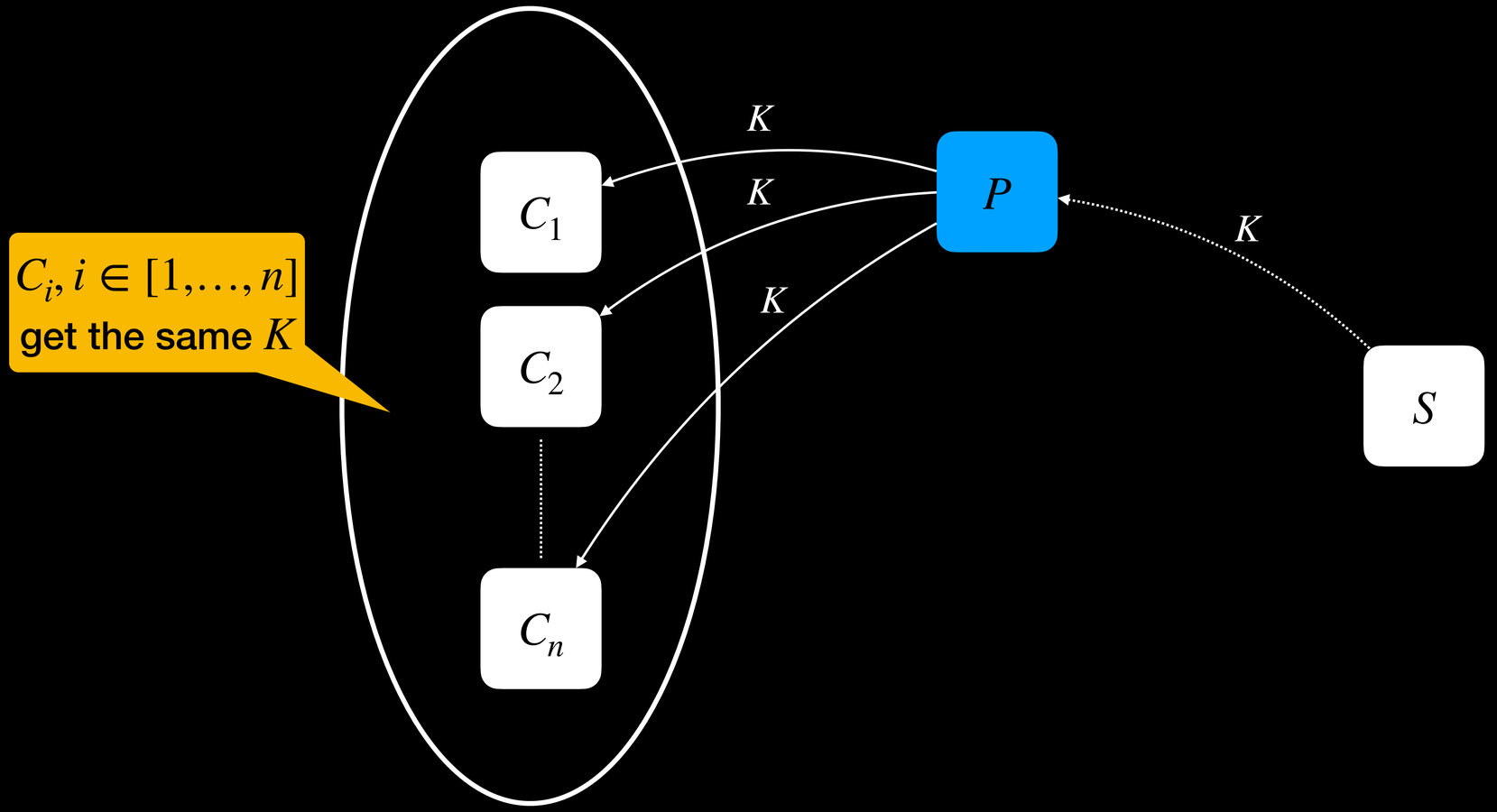
Fetch and verify through a trusted proxy

Fetch through multiple less-trusted proxies

Outsource to an audited or verified data store

Differing Approaches

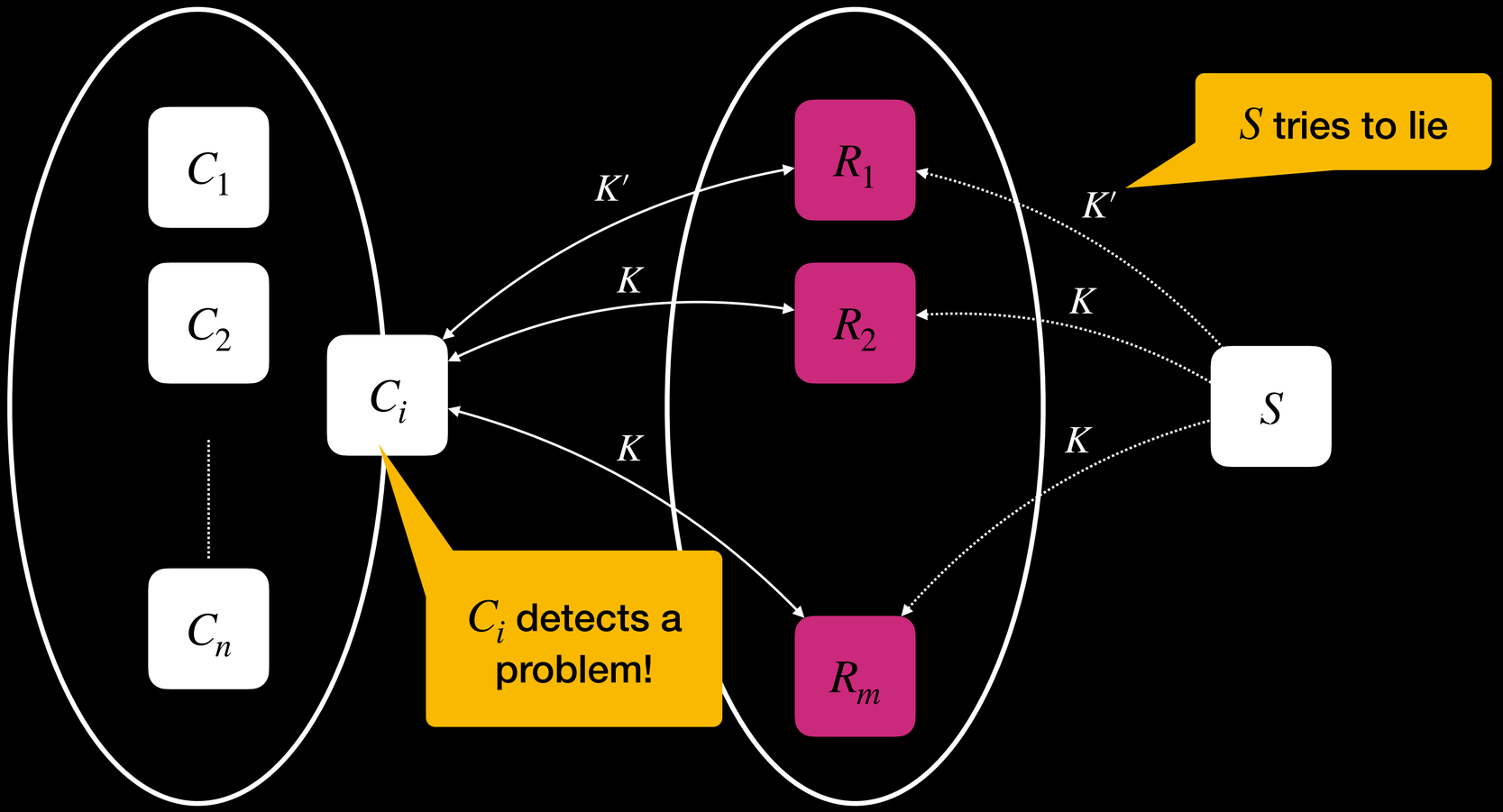
Trusted proxy discovery



Example: iCloud Private Relay key configuration

Differing Approaches

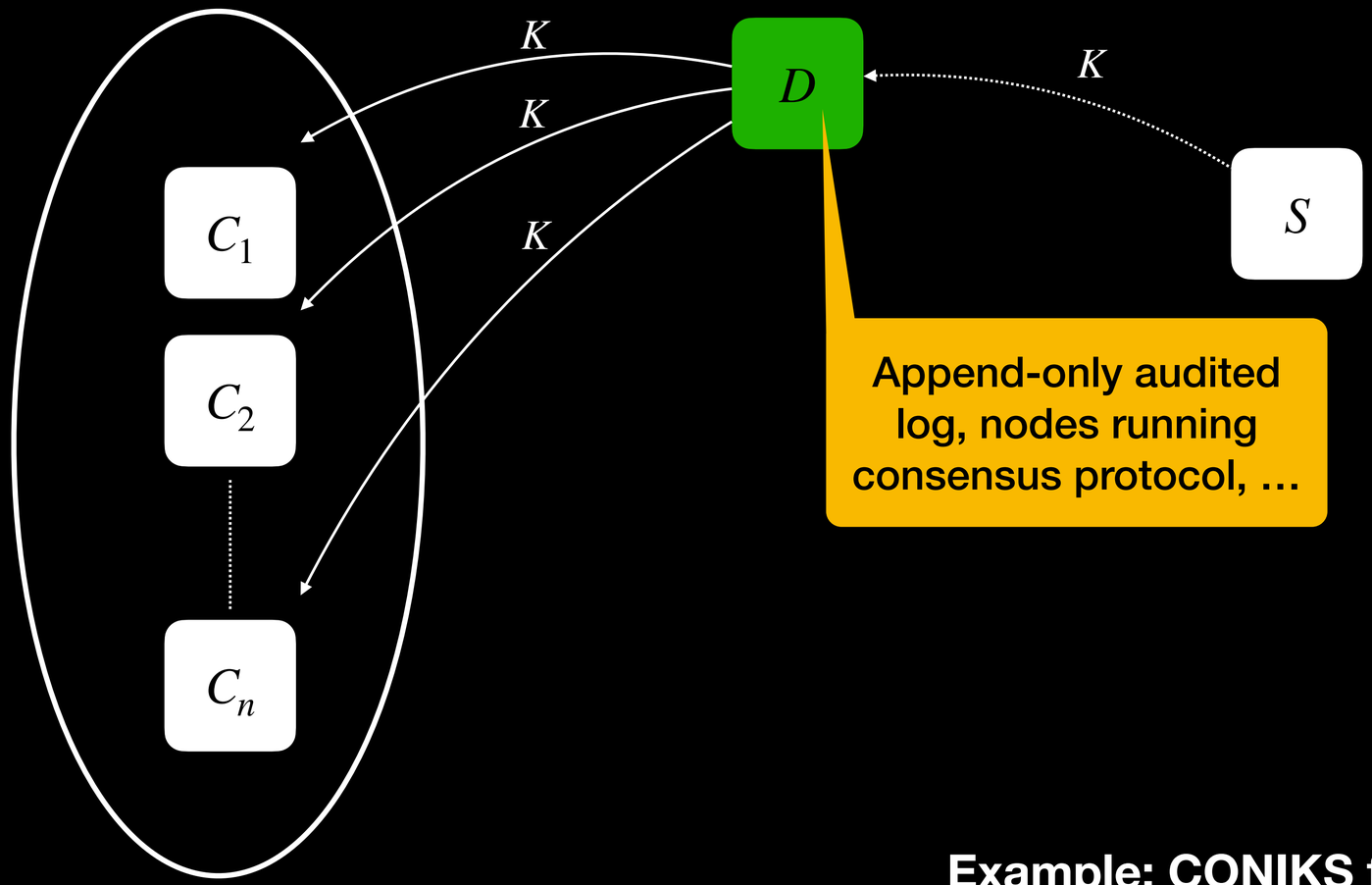
Multi-proxy discovery



Example: Consistency DoubleCheck

Differing Approaches

External database



Example: CONIKS for key transparency

Summary and Next Steps

Summary:

- Multiple unrelated protocols and applications share the key consistency problem
- All methods in the key consistency document describe architectures — not protocols — for enabling consistency

Next step:

Adopt as informational to complement deployed solutions and proposed specs (Consistency DoubleCheck)?

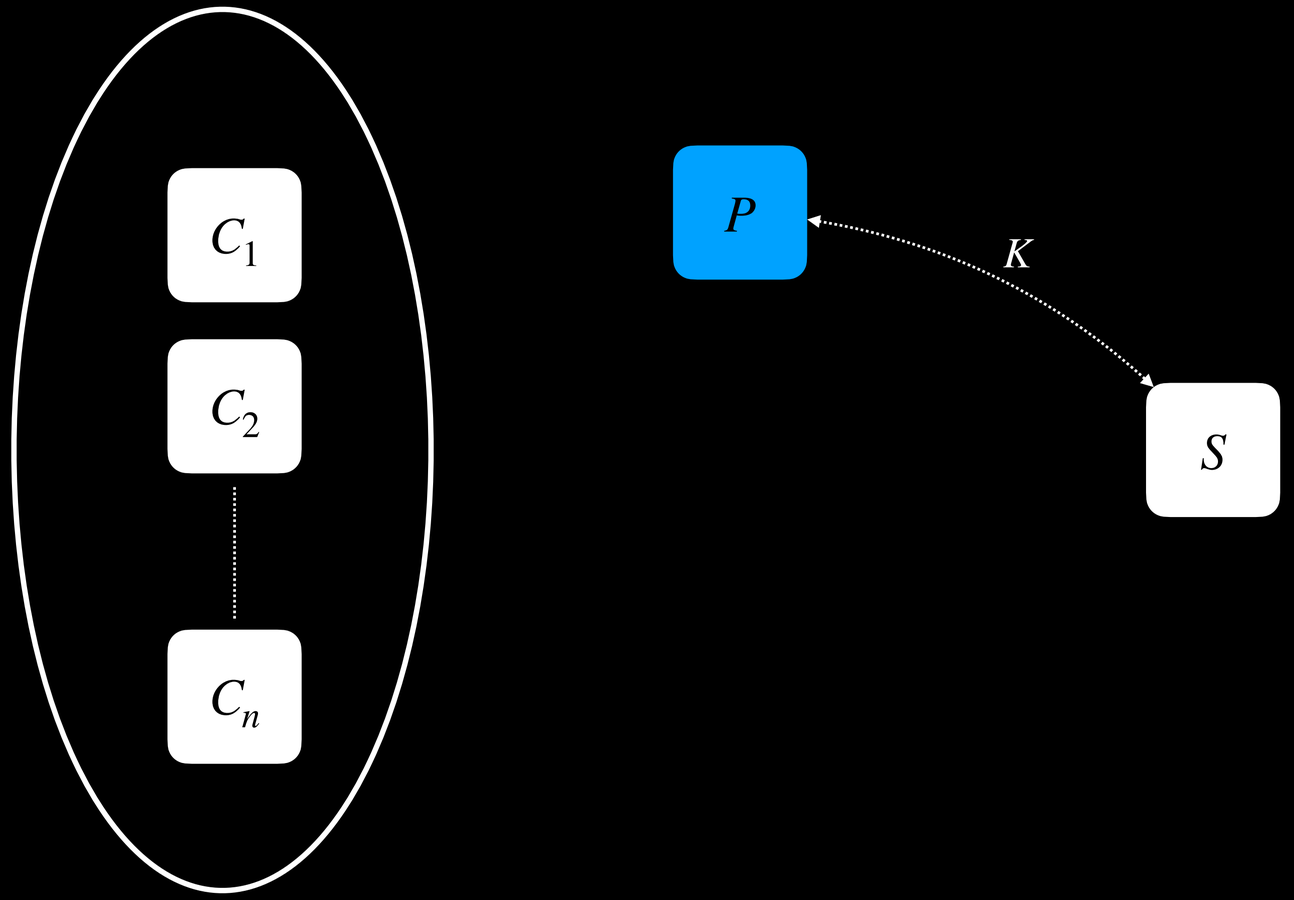
Key Consistency and Discovery

`draft-wood-key-consistency`

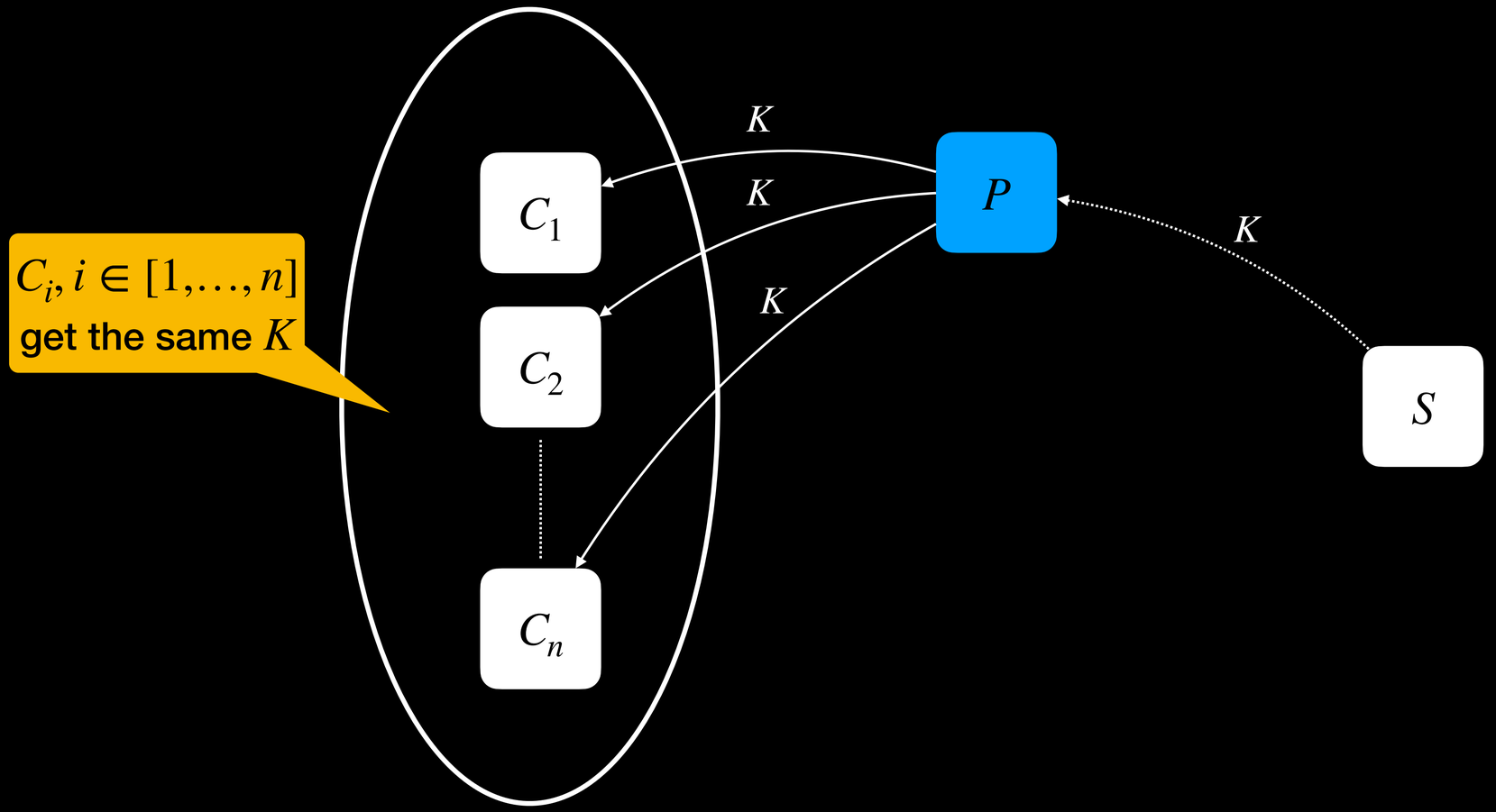
Davidson, Finkel, Thomson, Wood — IETF 114 — Privacy Pass

Backup

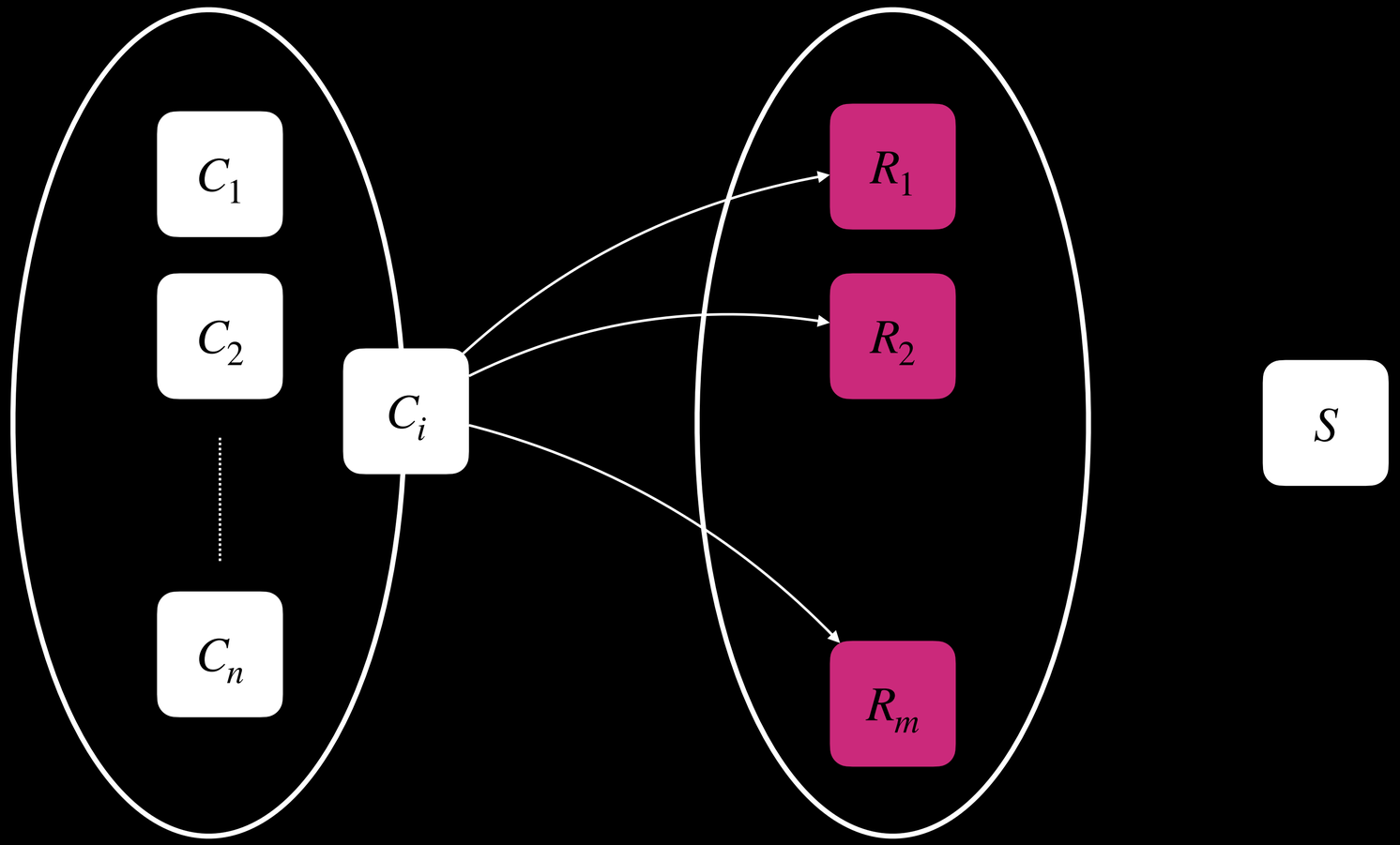
Trusted Proxy Discovery



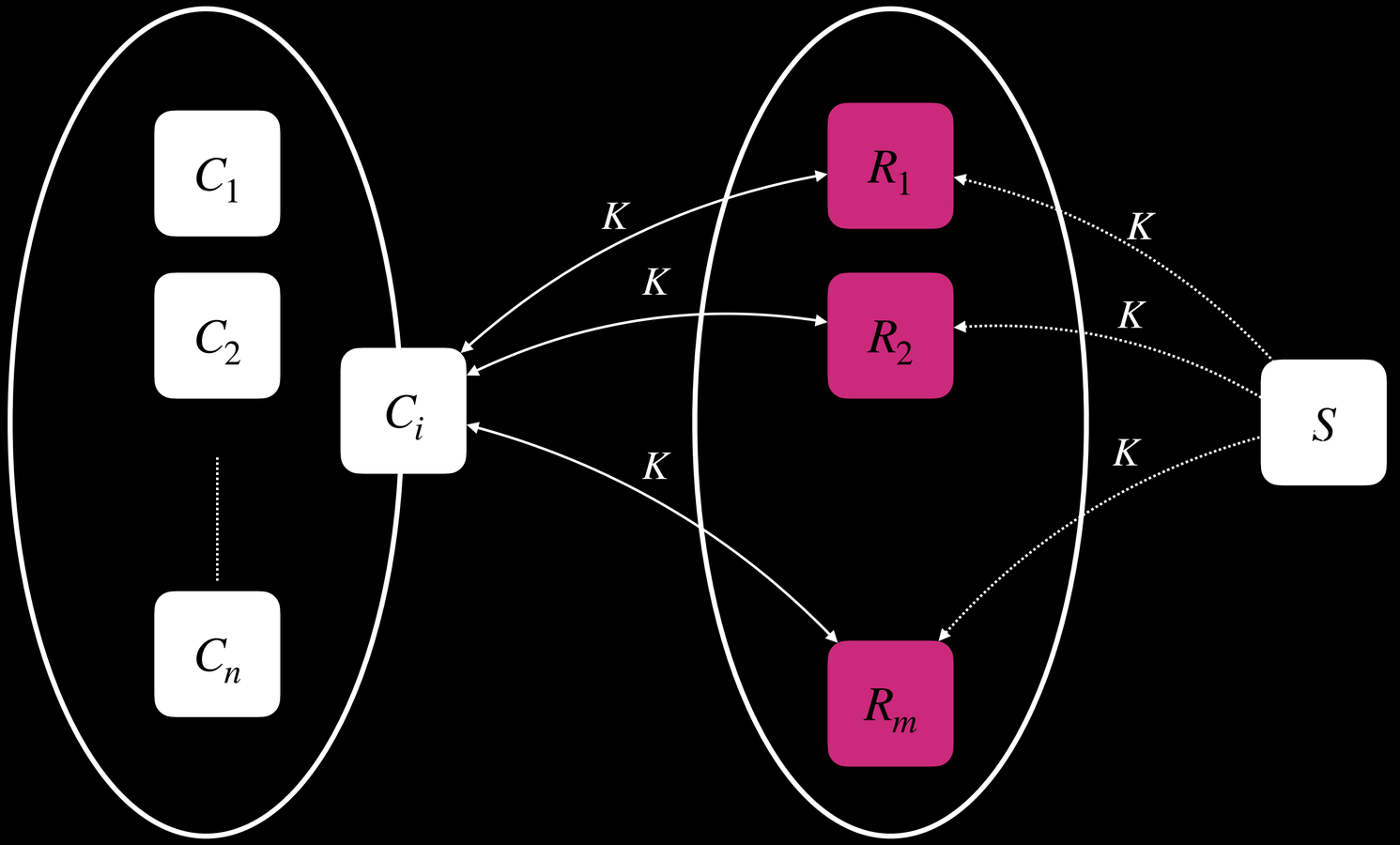
Trusted Proxy Discovery



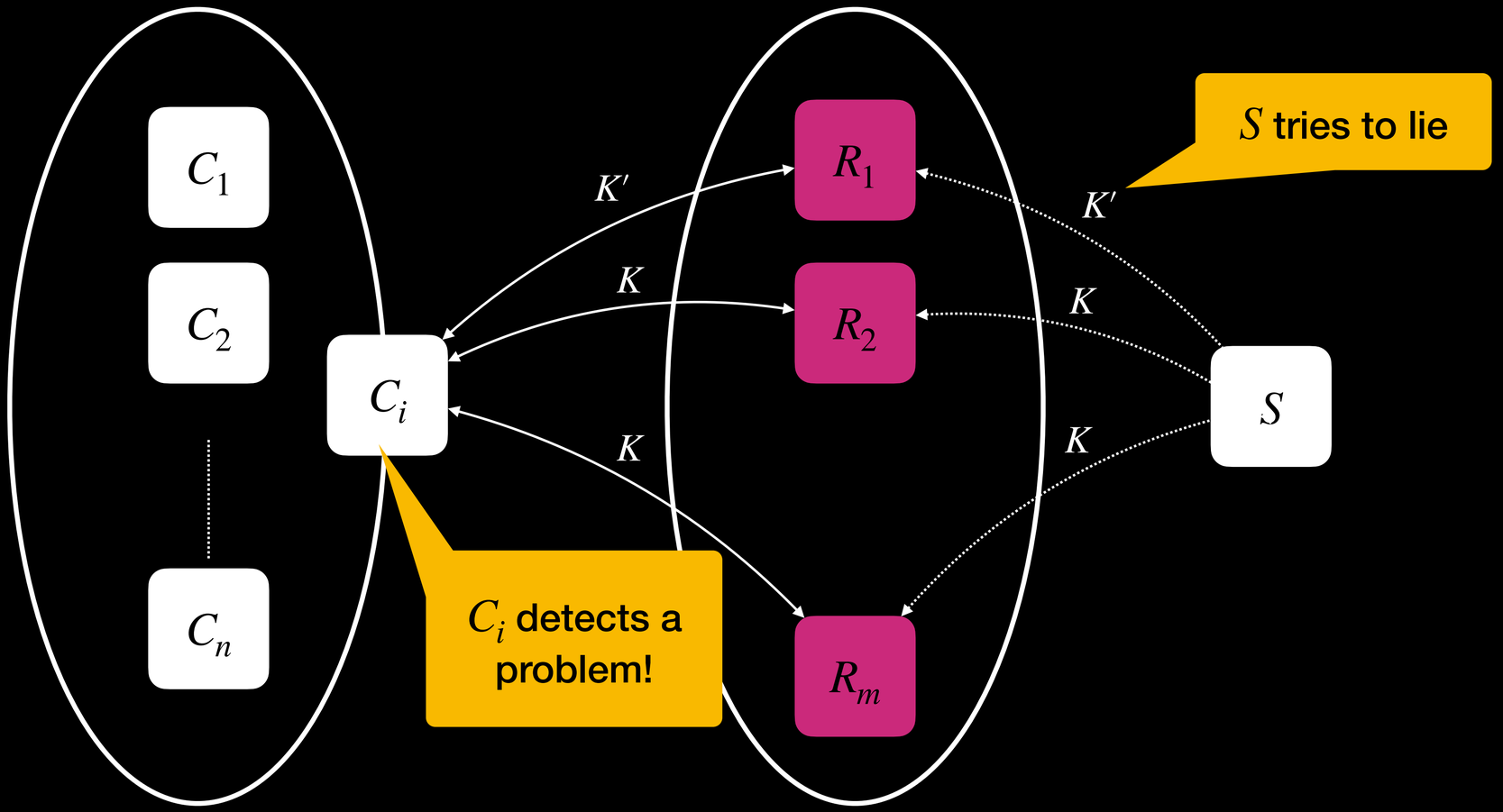
Multi-Proxy Discovery



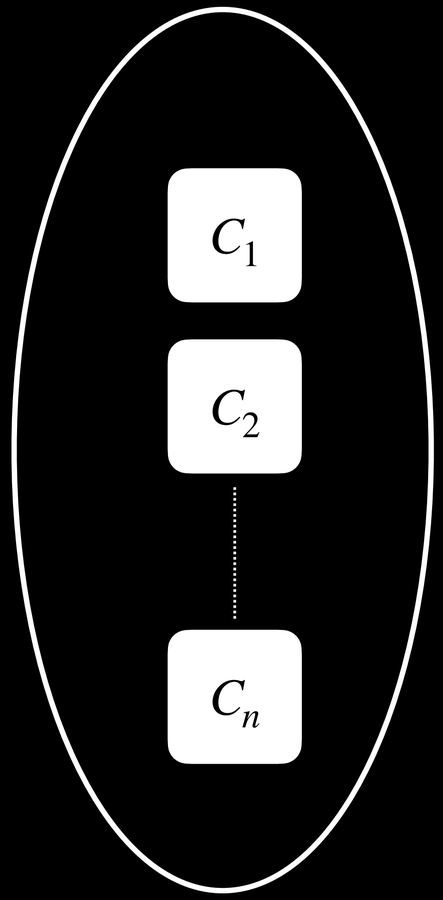
Multi-Proxy Discovery

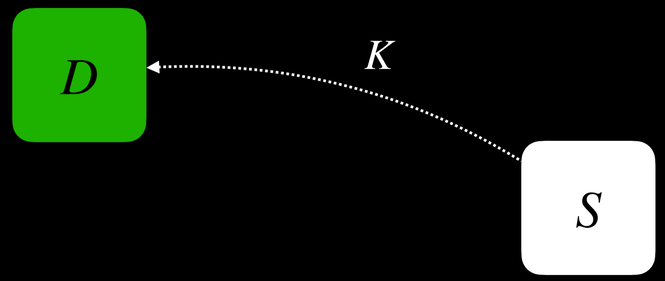


Multi-Proxy Discovery



External Database Discovery





External Database Discovery