Named Data Networking

NSF FIA PI Meeting
Berkeley, CA
May 25-26 2011

www.named-data.net

We are NDN

THE UNIVERSITY OF MEMPHIS

UCIrvine
University of California, Irvine

UCLA

Yale UNIVERSITY

Colorado State University

parc®
A Xerox Company

ARIZONA

UCSD

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Washington University in St.Louis

Agenda

A. NDN Overview

B. Two Initial Security Problems

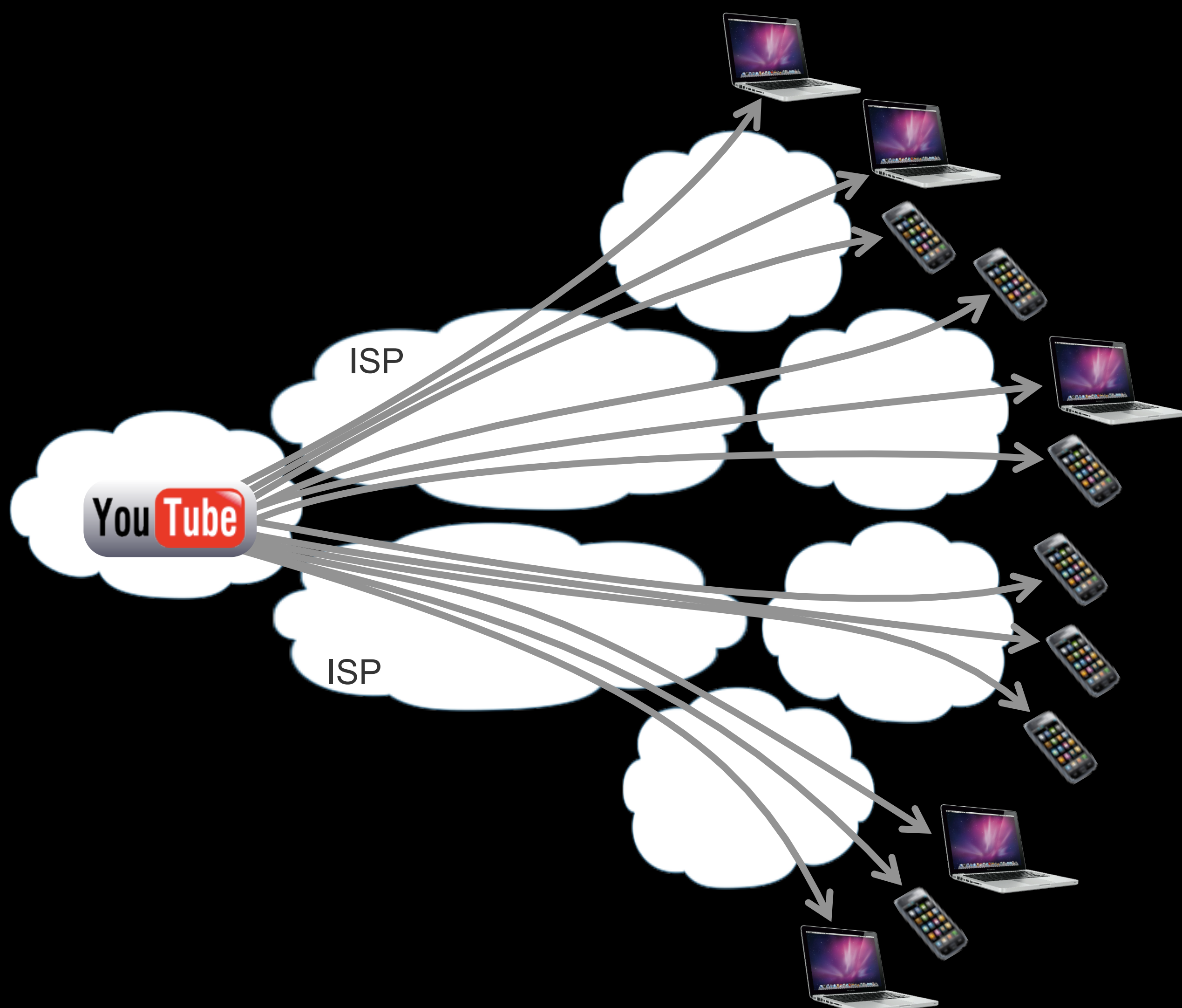
   1) Routing – OSPF

   2) Instrumented Environments – Lighting Application

C. Privacy Considerations

D. Summary

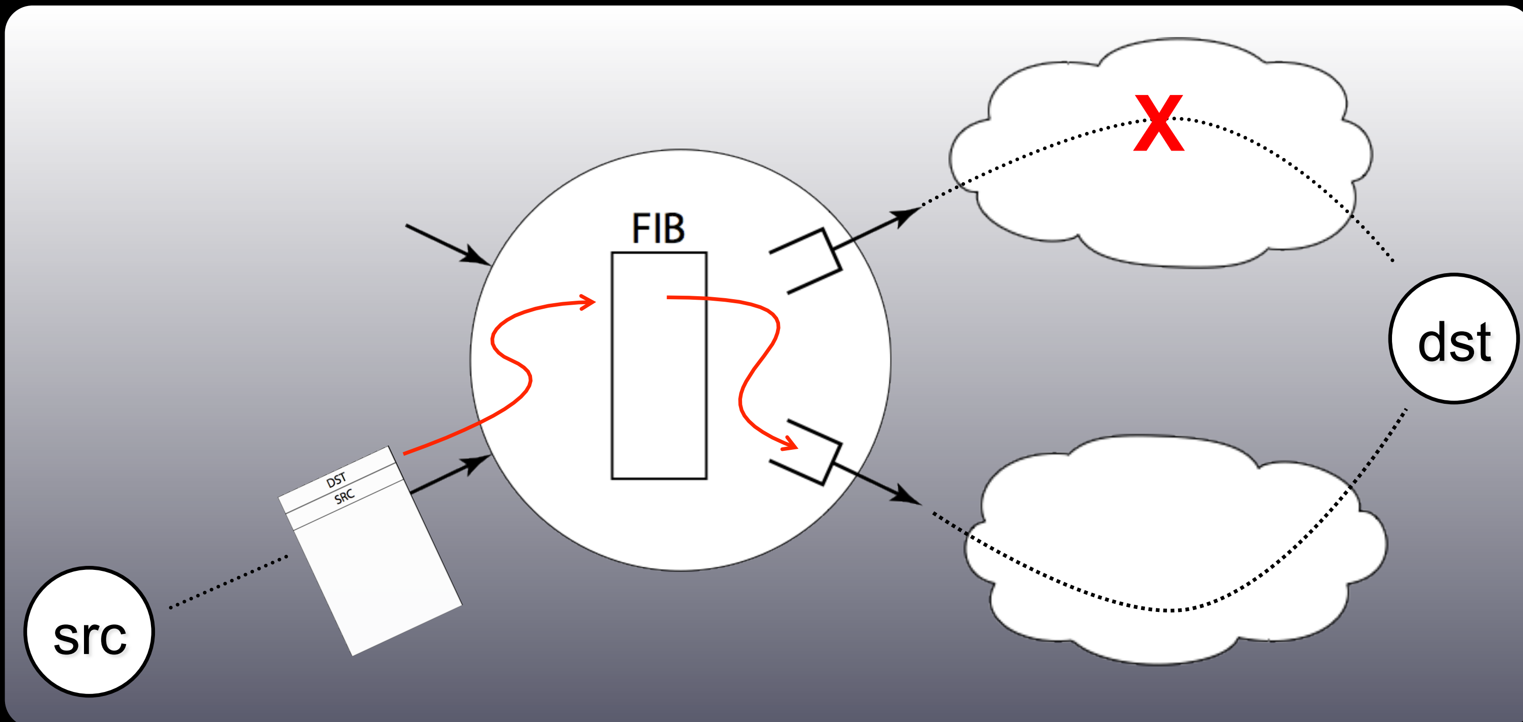
The problem



Communication v. Distribution

	Communication	Distribution
Naming	Endpoints	Content
Security	Secure Process	Secure Content

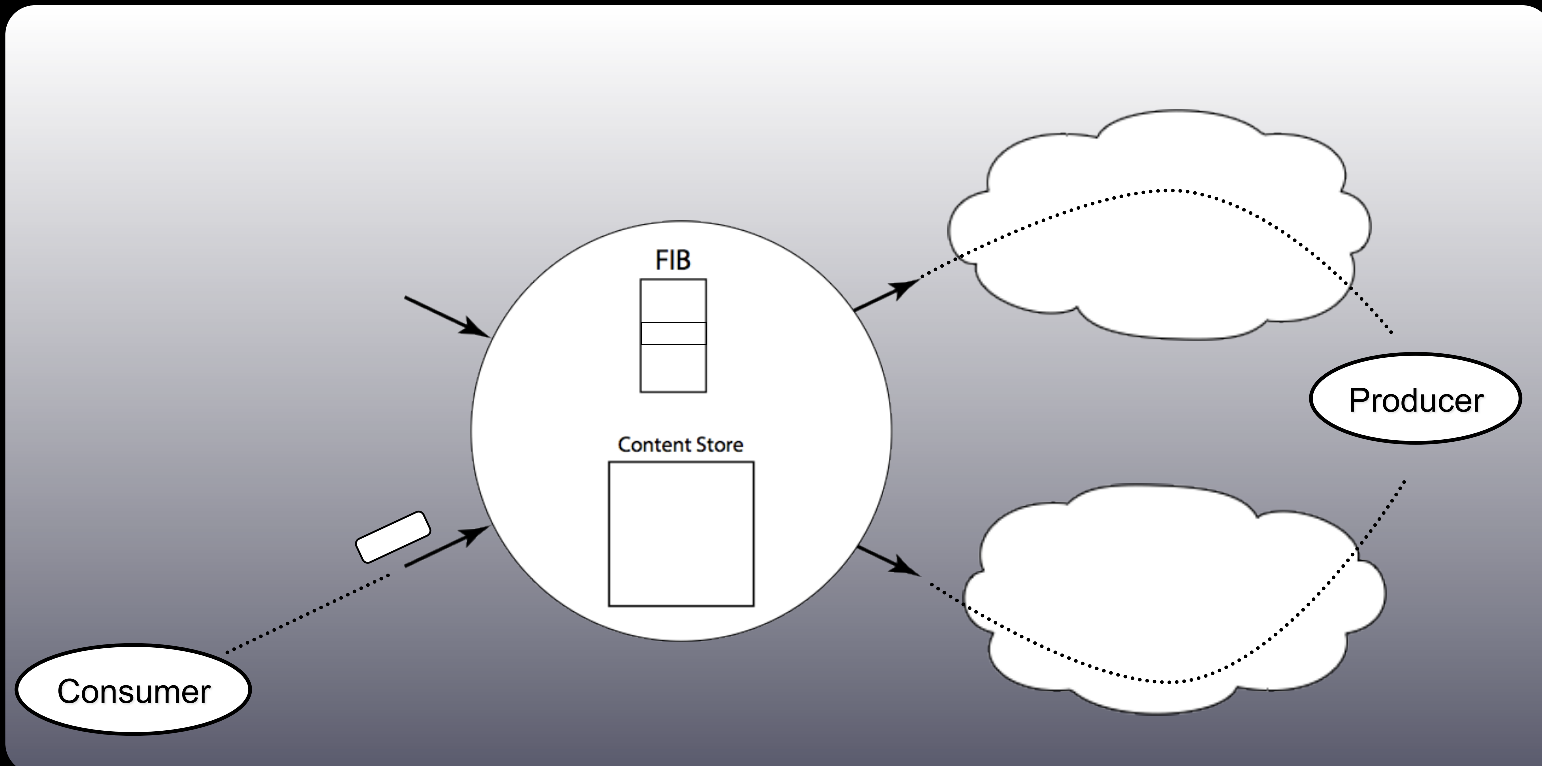
Today



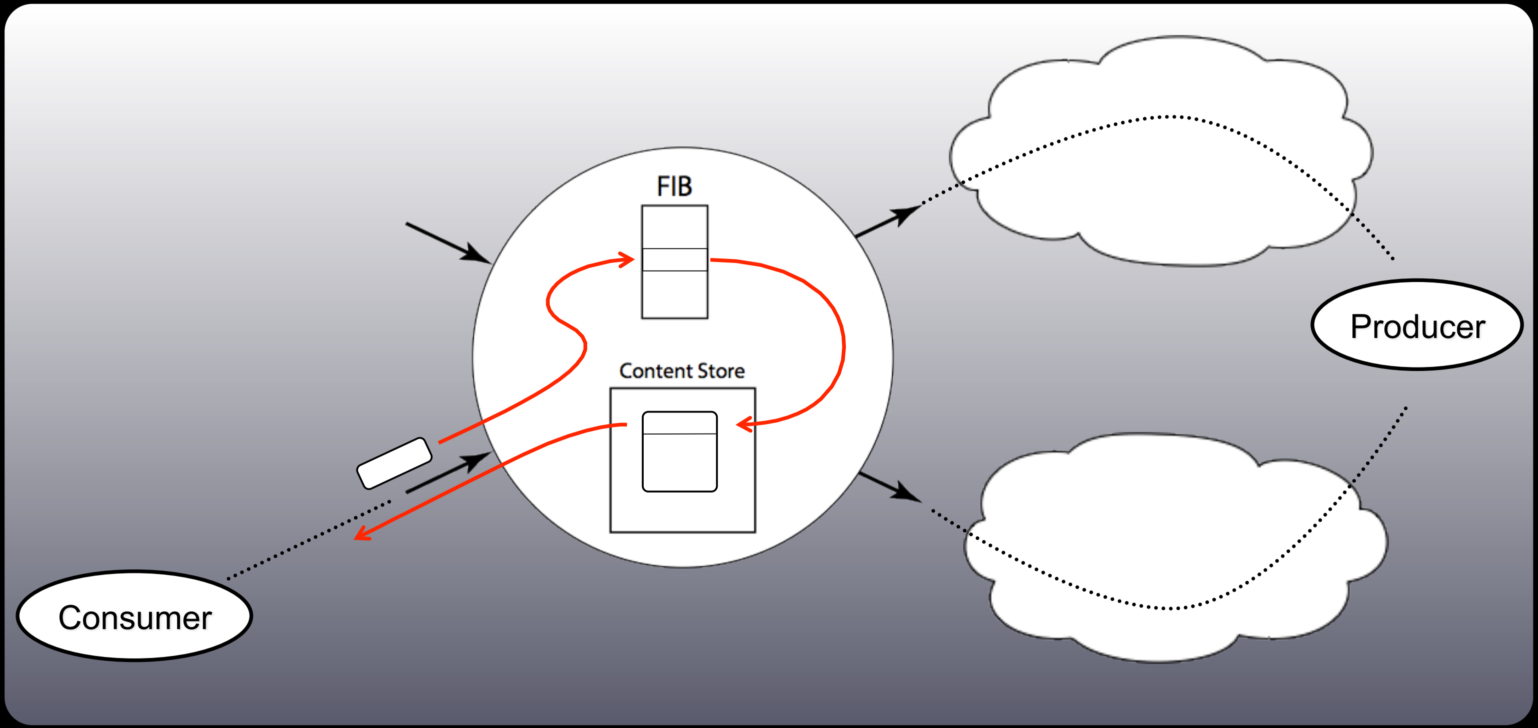
Path determined by global routing, not local choice

Structural asymmetry precludes market mechanisms and encourages monopoly formation

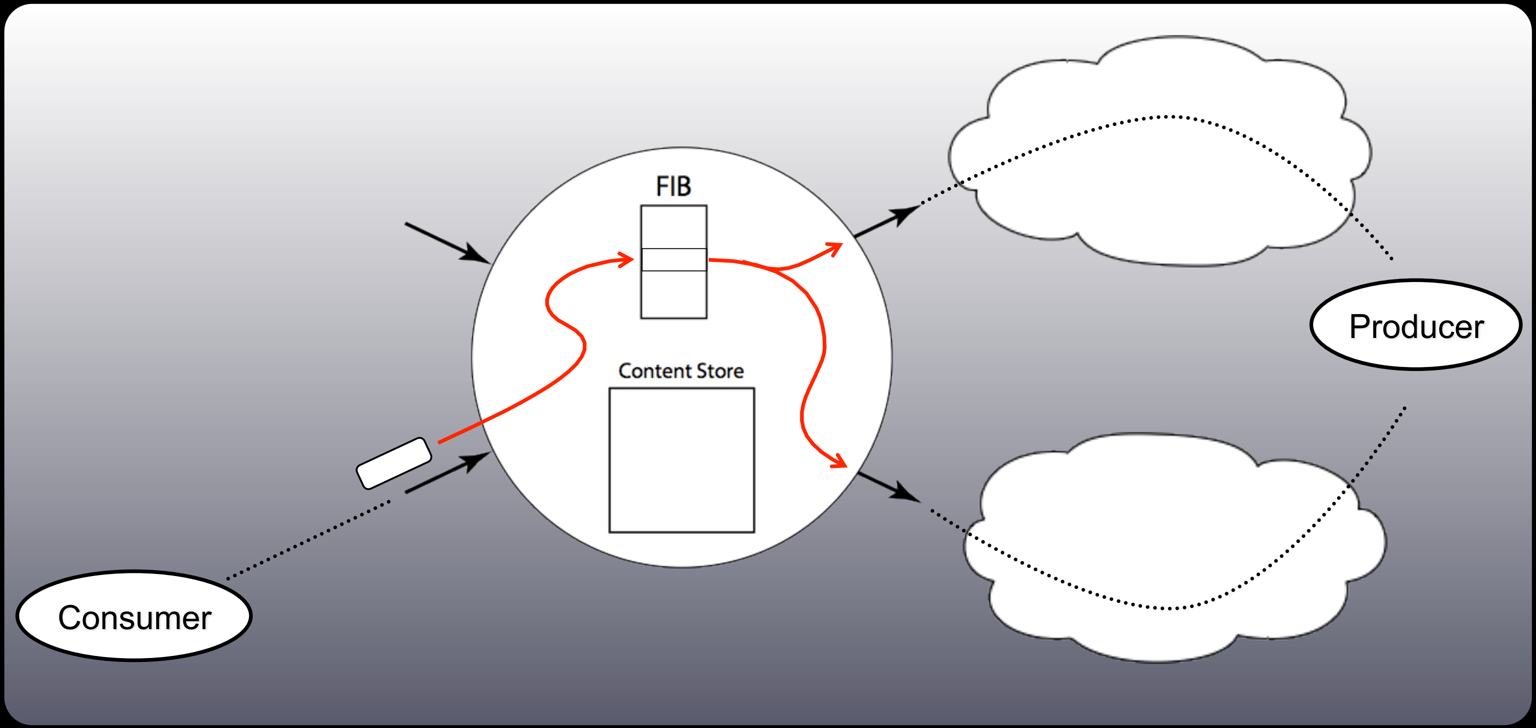
NDN approach



NDN approach

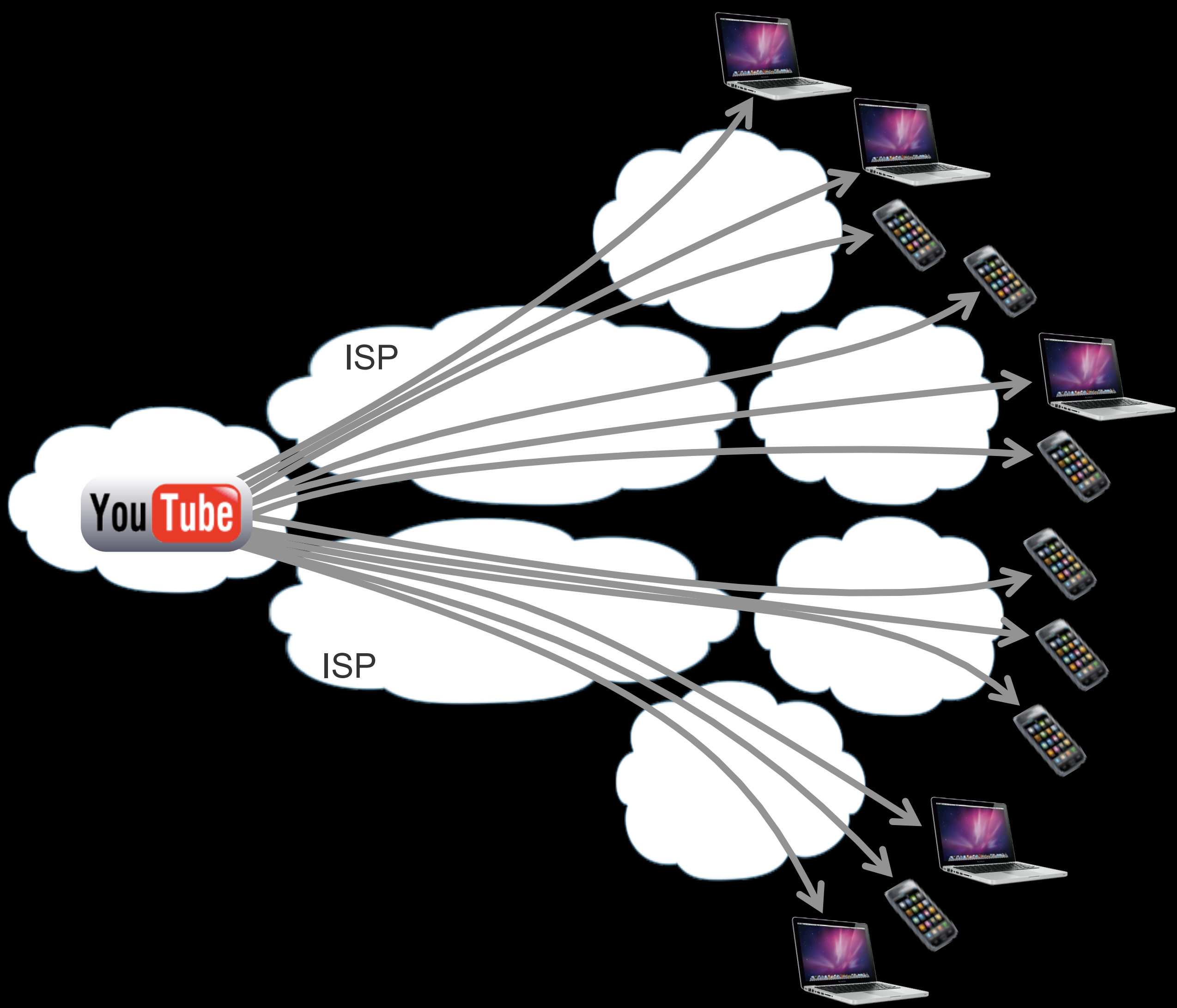


NDN approach

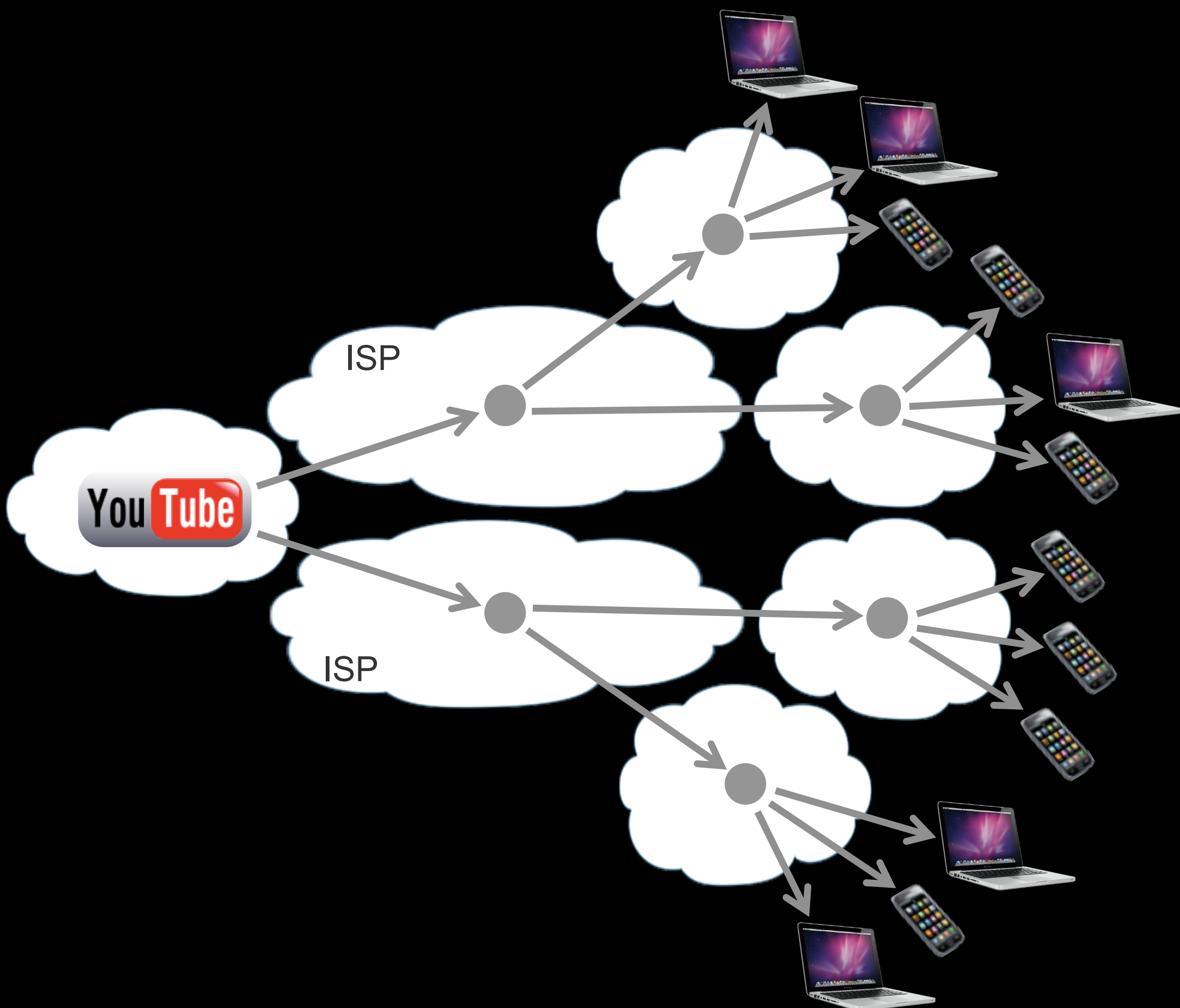


- Packets say 'what' not 'where' (no src or dst)
- Forwarding decision is local
- Upstream performance is measurable

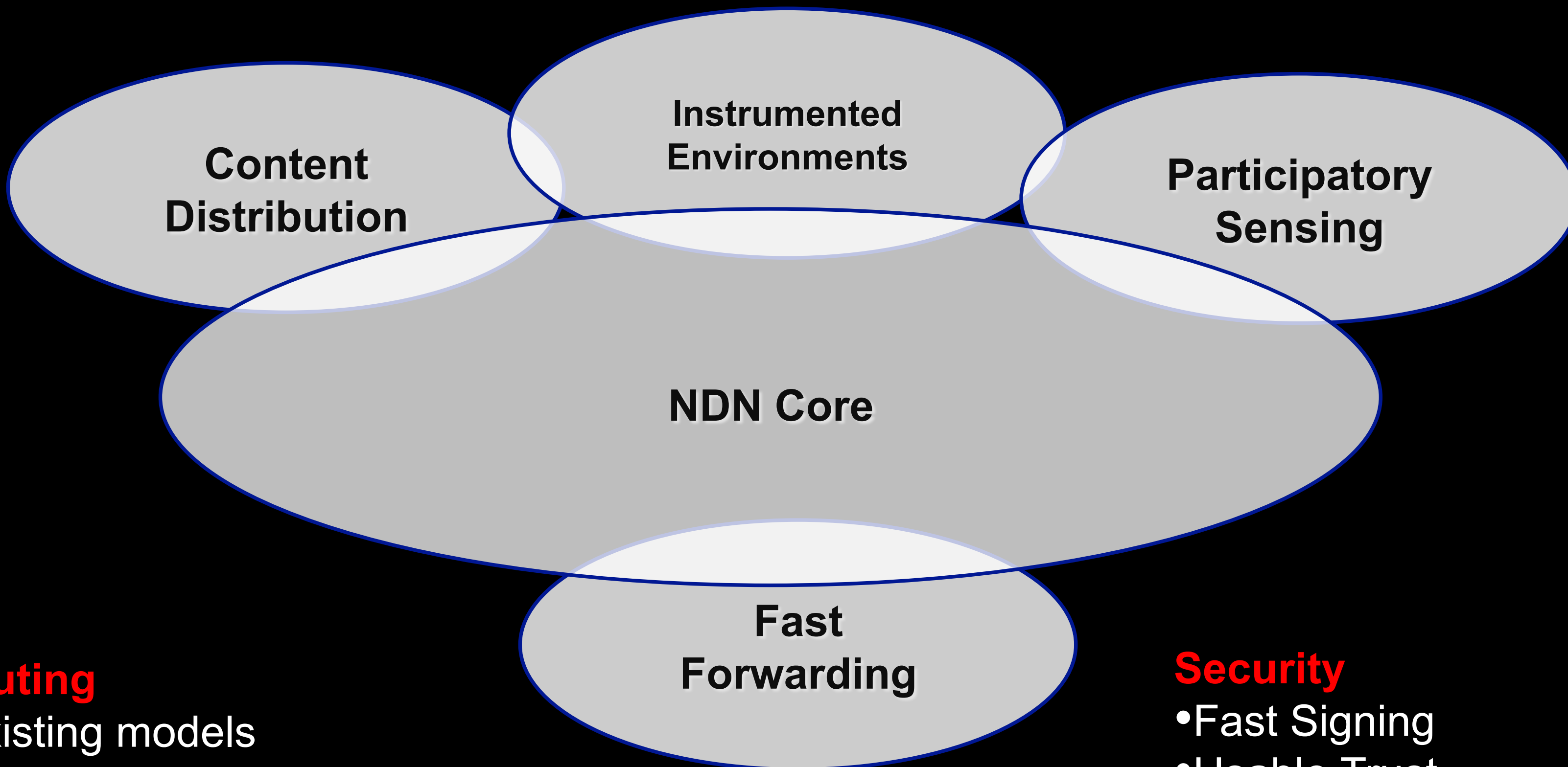
We envision replacing this:



With THIS:



Research Snapshot



Routing
- Existing models
- New models

Fundamental Theory
- Any-to-Any communication
- Bandwidth / Memory / Distance tradeoffs

Security
- Fast Signing
- Usable Trust
- Privacy
- Attack-resistance
- App. Security

Securing Content

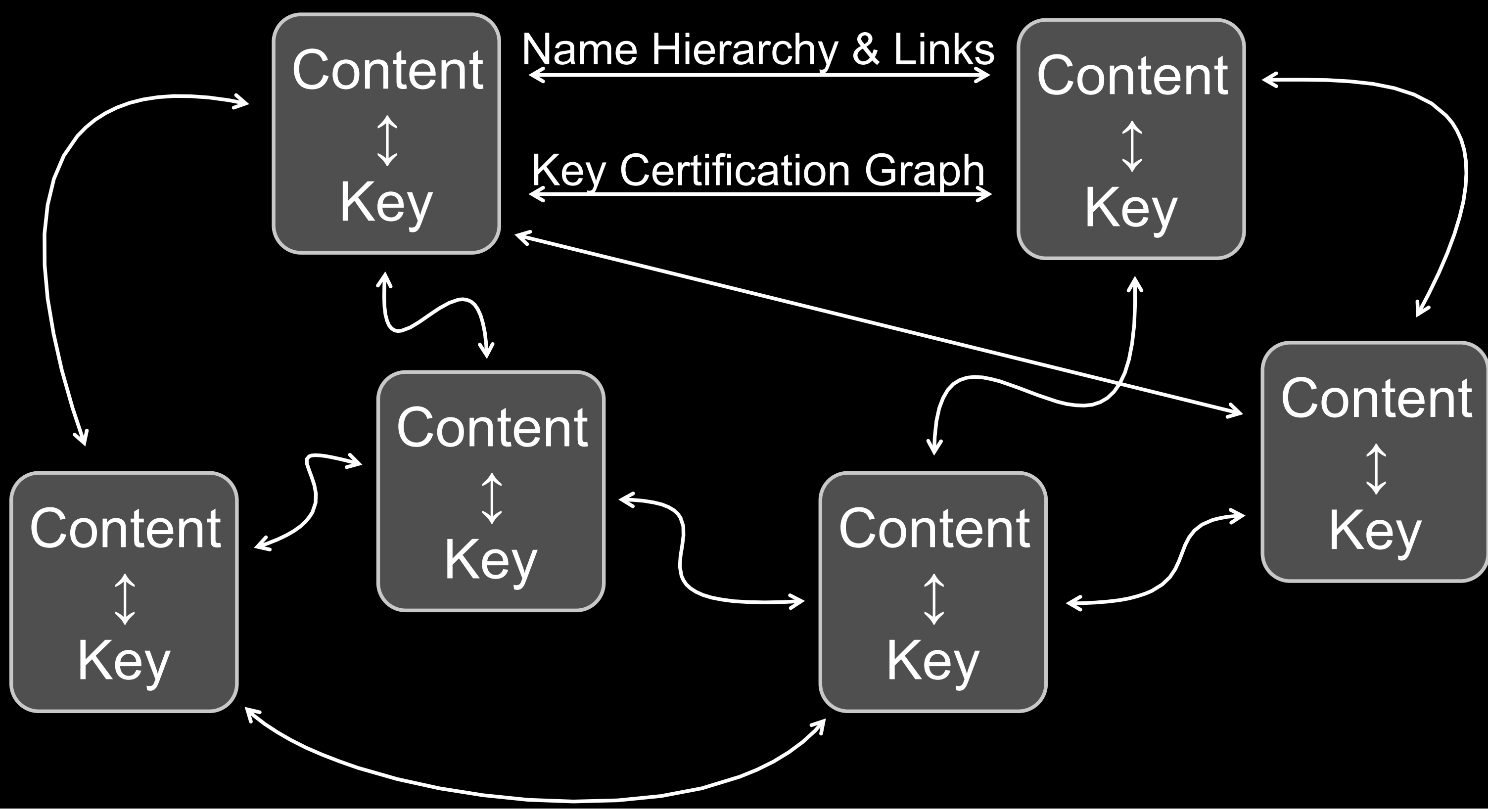
Content Packet = ⟨ *name, data, signature* ⟩

Any consumer can ascertain:

- Integrity: is data intact and complete?
- Origin: who asserts this data is an answer?
- Correctness: is this an answer to my question?

Evidentiary Trust

A web of trust gradually & organically arises from named and signed content:



Attack Resistance

Many current DoS + DDoS attacks/threats become irrelevant because of NDN architecture

- A few notable features:
  - Content caching mitigates targeted DoS
  - Content not forwarded w/out prior state set up by interests
  - Multiple interests for same content are collapsed

  - One copy of content per “interested” interface is returned

Agenda

A. NDN Overview

B. Two Initial Security Problems

   1) Routing – OSPF

   2) Instrumented Environments – Lighting Application

C. Privacy Considerations

D. Summary

Routing Security in NDN

We start with IGP (OSPF)

Routing Security with NDN

- Routing is a core function
  - A means to populate router FIBs
  - Routers exchange info about "where” content prefix is reachable
- How do we secure this process?
- NDN features help
  - Protect routing updates
  - Authenticity + integrity, freshness + timeliness, etc.

Data plane resilience

- IP data delivery strictly follows FIB direction:
  - One-way data flow -- cannot detect failures
  - Has no effect on routing decisions

- NDN content delivery is a 2-step process:
  - Interest forwarding to set up state
  - Content traversal of interest path in reverse
- Interest forwarding state eliminates looping, allows exploitation of topological redundancies and use of multipath interest forwarding
- Content packets measure quality of selected (interest) paths ➔ lets forwarding plane incorporate congestion and fault mitigation into path decisions
- If adversary is black-holing, forwarding plane can go around directly
- If adversary sends false data: nodes that verify signatures (routers or end-nodes) can inform the forwarding plane to go around adversary

Using NDN Security Features

- Router names follow network management hierarchy
- Names associated with signing keys (not only 1:1)
- Keys are authenticat-able:
  - Network operator configures trust anchor for each router, e.g., public key for /ndn/ucla.edu/
  - Router key (e.g., /ndn/ucla.edu/bb1) certified by anchor key
  - Each interface has a name, (e.g., /ndn/ucla.edu/bb1/f1); router key certifies each interface key
- Updates from each interface signed by that interface key

Agenda

A. NDN Overview
B. Two Initial Security Problems
   1) Routing – OSPF
   2) Instrumented Environments – Lighting Application
C. Privacy Considerations
D. Summary

NDN Lighting Control Application

Testbed: UCLA Film & TV Studio #1

- Special case of actuators in an instrumented environment
- Rich set of use cases (e.g., entertainment)

IP in Lighting Systems?

- Security currently achieved by:
  - Physical network segregation, or
  - VLANs + firewalls
- Devices increasingly receive over-the-air upgrades & updates
  - Not clear how to accommodate with above in scalable manner
- IP-based addressing irrelevant to applications
  - Easier to address fixtures in application-specific terms without having to know through/to which gateway they connect
- IP configuration particularly brittle for dynamic systems
  - Lighting devices (fixtures) can come & go frequently
  - Certain building systems incorporate mobile devices

NDN for Lighting Control

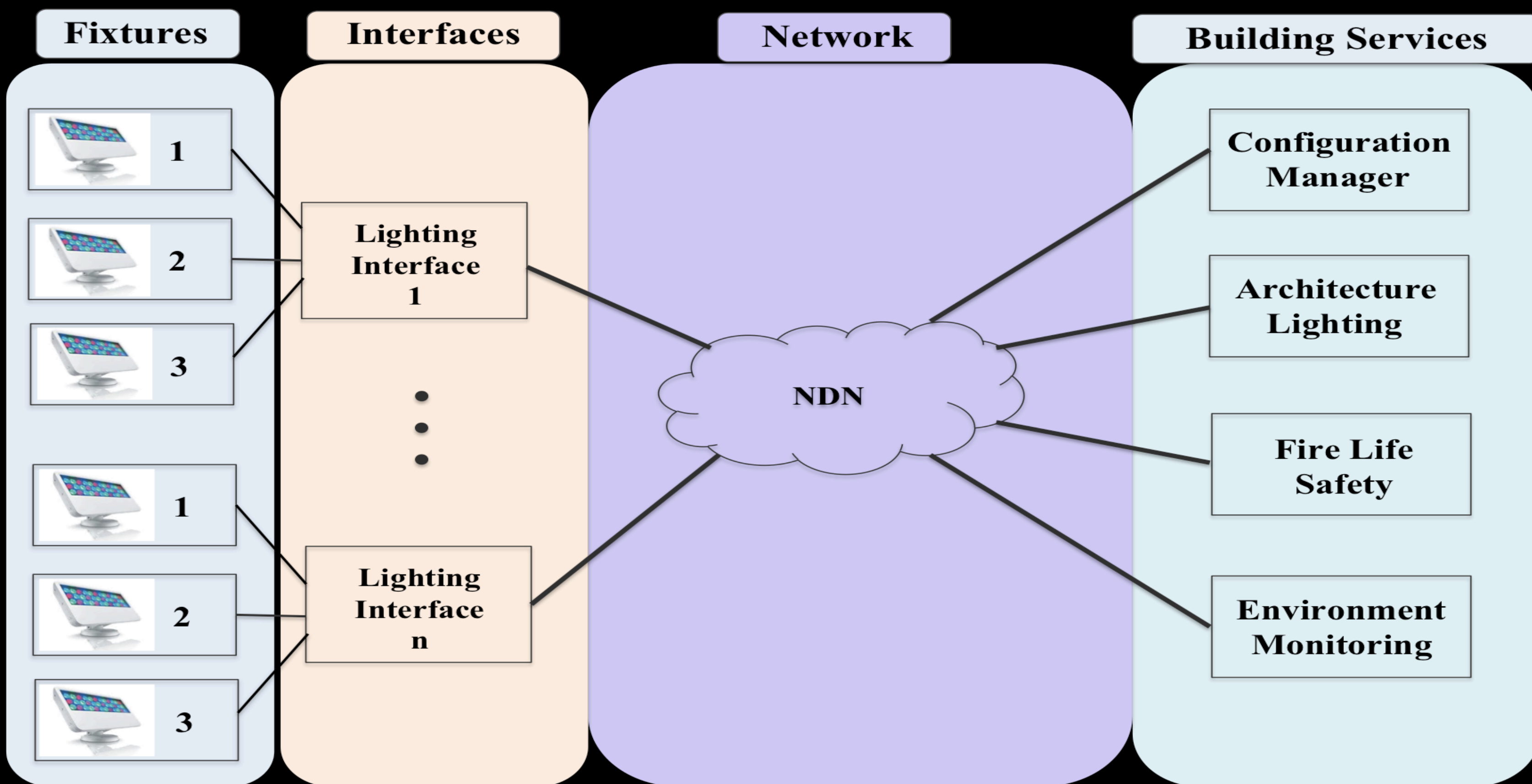
Two challenges: Configuration and Control

Design goals

- No IP-like configuration issues
- Application-assigned meaningful names
- Secure enough to use over Internet
- Multiple controlling applications with different capabilities
- Scalability (many fixtures!)
- Quasi-real-time performance (ca. 50ms response time for now)

✓ Industry-standard LED lighting by Philips Color Kinetics
  - ✓ Commonly used in architectural and entertainment settings.
  - ✓ IP and Ethernet for fixture & power supply discovery, configuration & control

Multiple Controlling Processes



NOTE: Every entity has a public/private key-pair, including:
fixtures, power supplies, embedded interfaces and applications

Bootstrapping

- No preconfigured information in fixture, other than manufacturer-supplied:
  - Public/Private key-pair
  - Initial authenticator

- Standard mechanisms used for lighting interface to connect to NDN on one side and discover fixtures on another

- Fixture starts with pre-configured name:

  /ndn//lighting/<manufacturer>/<Pubkey-hash>

- To discover fixtures, configuration manager sends interests for:

  /ndn/lighting/

  - Once located new fixture, retrieves (via interest) its public key data:

    /ndn/lighting/<manufacturer>/<Pubkey-hash>/key

  - Out of band, application obtains initial authenticator & fingerprint of public key per fixture

- Configuration manager issues “signed interest” authorizing its public key to configure fixture
  - Contains KeyLocator for configuration manager public key
  - Includes initial authenticator of fixture, encrypted with latter’s public key

Control

- After bootstrapping, configuration manager grants permissions to applications by publishing their keys under names representing (authorized) capabilities
- Signed by key already authorized for fixture:

  <app-key, capability, authorized-key>

- Fixture checks if application signing key is in:

  (1) its cache of authorized keys, or (2) built-in trust anchor list created at bootstrap time

  If in neither, fixture issues interest for:

  <path-to-key>/authority/<name-used-to-access-fixture>/<capability>

  and checks that corresponding content signed by an authorized key

Control via Signed Interests

- Application initiates control actions: need to minimize delay
- Capabilities (commands): name, configure, control, read and override
- Expressed as part of name within interest
- Application issues *signed interest*
  - signs empty content with appropriate name
- To prevent replay, includes counter (or timestamp)
- Fixture replies with content representing ACK or current state

Synchronized control of multiple fixtures via fixture-issued long-lived interests

Agenda

A. NDN Overview

B. Two Initial Security Problems

   1) Routing – OSPF

   2) Instrumented Environments – Lighting Application

C. Privacy Considerations

D. Summary

Communication Privacy

- Interest:
  - Generally does not say where it will end up
  - Away from consumer: says nothing about who requested content
  - Close to consumer (Alice): leaks name of requested content (Bob's video)
- Content:
  - Does not say where it is coming from now
  - Traditional signatures leak origin (producer)

Whither Name Privacy?

NDN names are expressive and meaningful, but…

- Leak information about requested content
- Can make it easy to filter, e.g., block all content to/from:

  /ndn/cnn/world-news/china/

However:

- NDN names are opaque to network
  - Routers only need to know name component boundaries
  - Names can carry binary data

Name Privacy Requirements

- Observers close to consumer should not learn what is being requested
  - Name in interest needs to be hidden
  - Content name and signature must not leak origin
- Consumer needs to verify content signatures
- Consumer hiding its identity from producer
  - Already provided by NDN – does not require encryption

Anonymization Services

- Usually done at higher layer(s)
- Consumer picks a set of anonymization servers
- Only last server learns name in interest
- Content encapsulated/encrypted and routed back
- Drawback: suboptimal routing

- Can also be done at NDN layer (see below)

General Approach

Flexible name encryption:

- Consumer picks components to encrypt
- Names with encrypted components adhere to NDN syntax, e.g.,

/ndn/uc/ E_{UC}(uci) /staff/ E_{UCI}(cs/Alice/blog/) / today/joke

- Each router offering this service advertizes its public (encryption) key
- Public keys are namespace-specific

Routing Encrypted Names

- Concentric encapsulation
- Full encapsulation (akin to anon. services)

Caveat: what's good for privacy, not always so for security. Encrypted names in interests:

- Inhibit collapsing interests in routers
- Can prompt DoS possibilities

Concentric Encapsulation

/ndn/uc/uci/cs/Alice/blog/today/

/ndn/uc/E_{UC}(uci / E_{UCI}(cs/Alice/blog/today/, k))

- Last decrypted component carries symmetric key
- Decrypting routers replace signatures on content
- Consumer receives original producer signature
- Separate from content encryption

Full Encapsulation

/ndn/uc/uci/cs/Alice/blog/today/

↓

$X=E_{YALE}$(/ndn/uc/uci/cs/Alice/blog/today/, k)

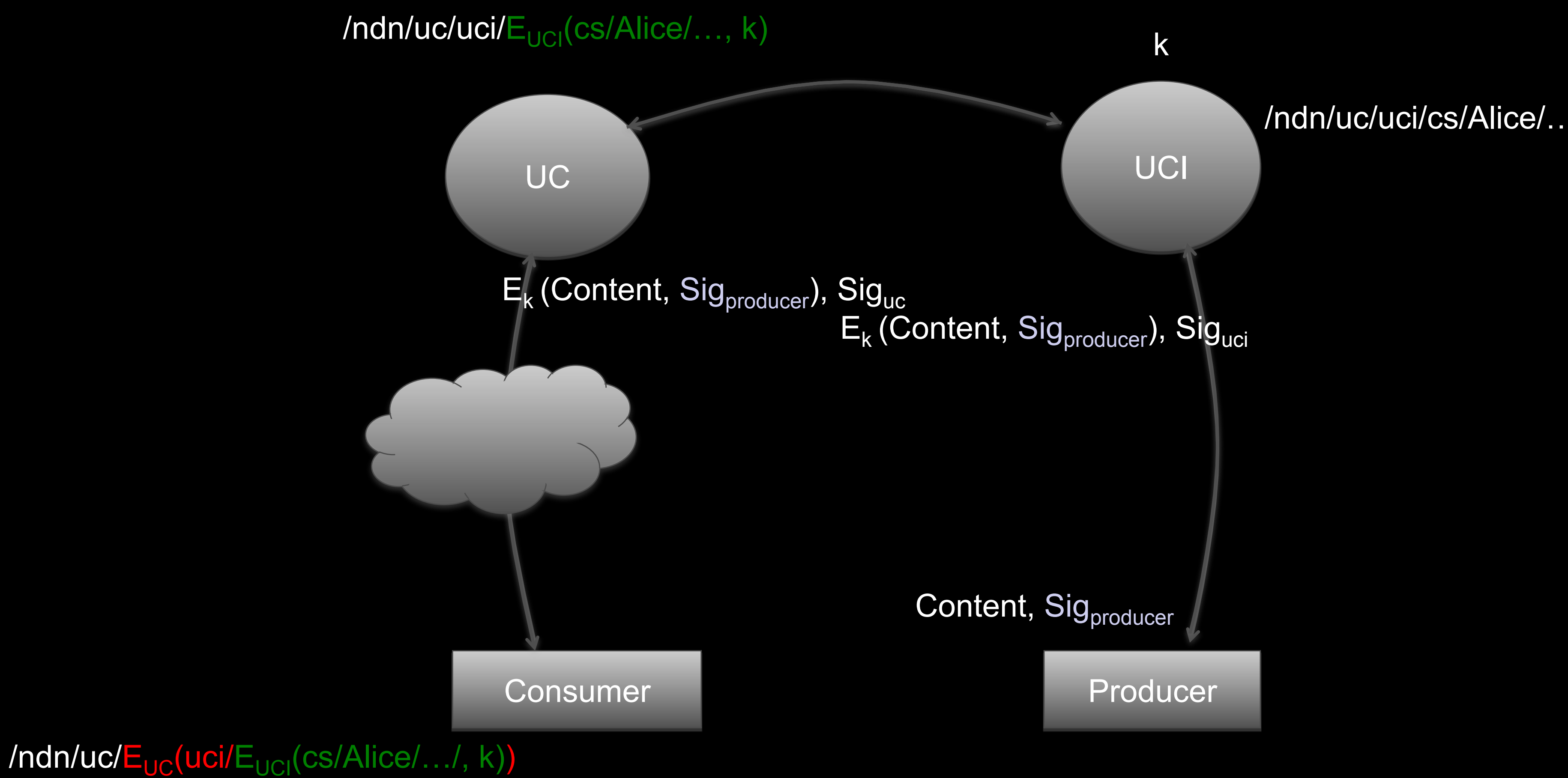
↓

$Y=E_{WASHU}$(/ndn/yale/anon/X, k')

↓

/ndn/washu/anon/Y/

Concentric Encapsulation



Agenda

A. NDN Overview
B. Two Initial Security Problems
   1) Routing – OSPF
   2) Instrumented Environments – Lighting Application
C. Privacy Considerations
D. Summary

SUMMARY

- Lots of work underway
- Much of what was presented not “cast in stone”
- Didn’t cover:
  - Signature schemes (e.g., batch operations, streaming content)
  - Trust establishment / Trust frameworks
  - Usability of S&P
  - Security in other apps, e.g., sensing, conferencing