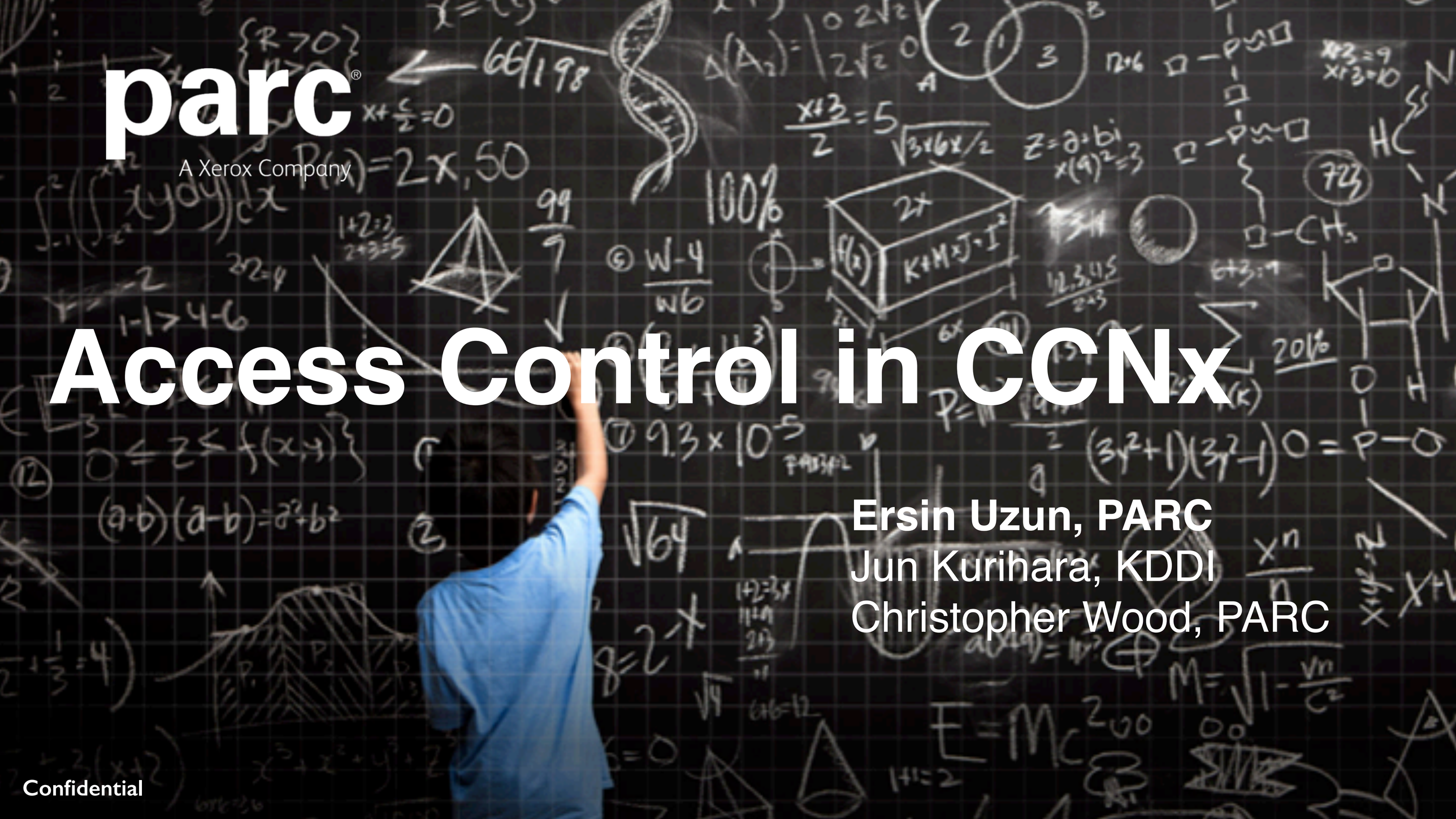


parc®
A Xerox Company

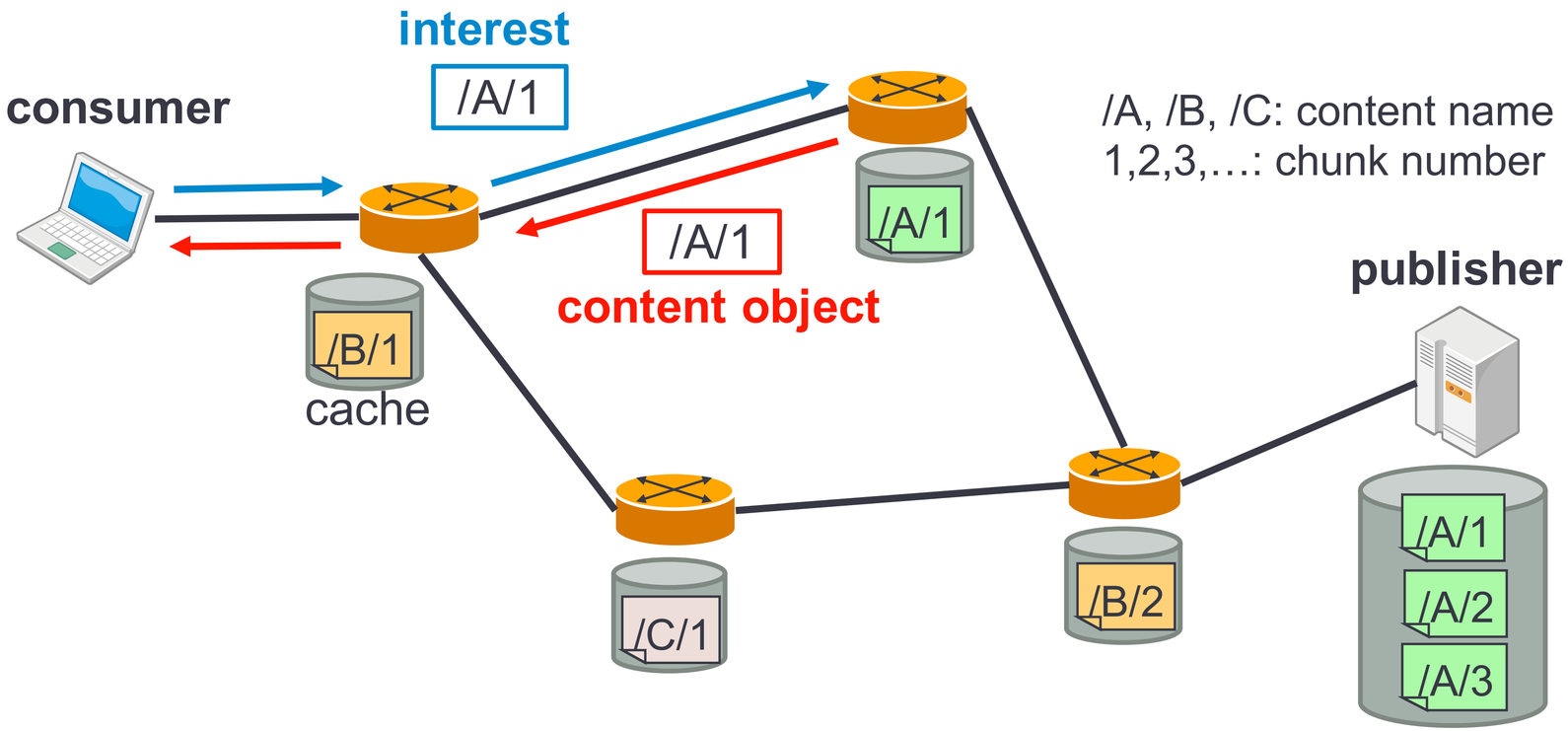
# Access Control in CCNx

**Ersin Uzun, PARC**
Jun Kurihara, KDDI
Christopher Wood, PARC

# Agenda

1. Motivation
2. CCN-AC: Encryption-Based Access Control Framework for CCN
3. Instances of CCN-AC
4. Conclusion

# CCN Overview






parc
A Xerox Company

# Access Control in CCN

Essential:

- Producers need ways to ensure that content can only be accessed by authorized consumers

Non-trivial:

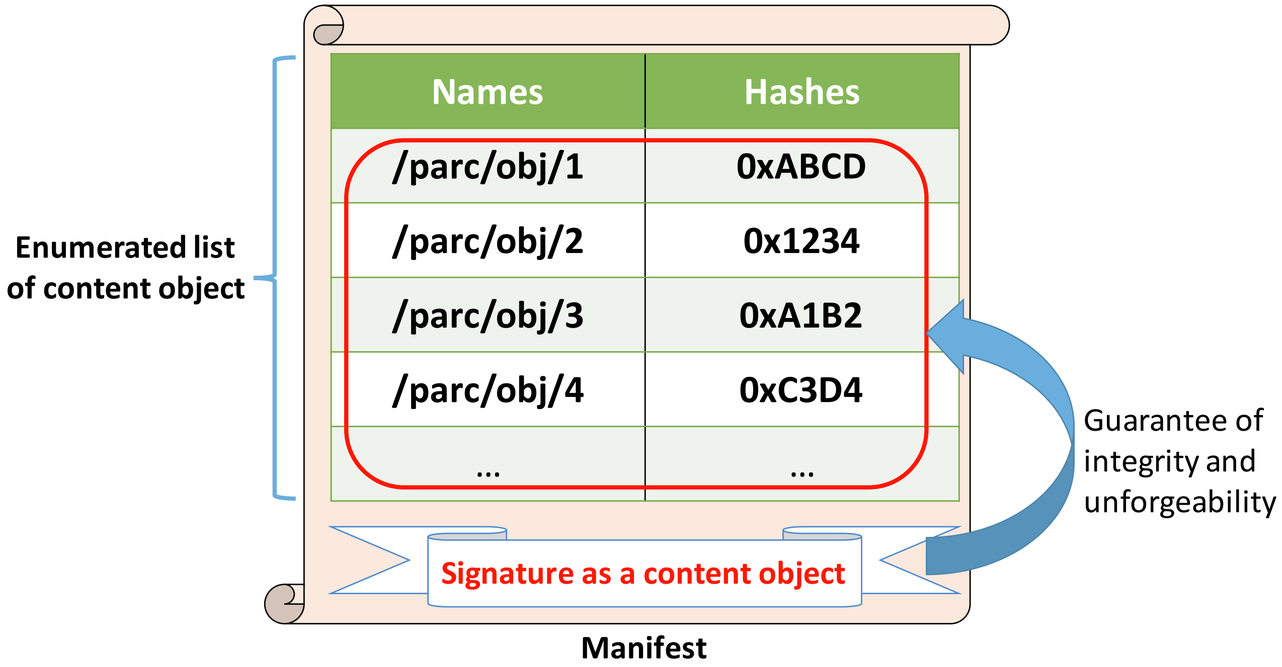
- It should not invalidate caching benefits
- It should be secure, flexible, scalable and easy to use

# CCN-AC: Encryption-Based Access Control

# CCN 1.0 Manifest Structure

Manifests encapsulate a list of interest names and hashes

The Manifest signature guarantees the integrity of each listed item






parc
A Xerox Company

# Manifest-Based Content Retrieval

Content retrieval process:

1. Obtain the manifest

2. Issue interests for referenced Content Objects

3. Check the validity of received responses —via Content Object hashes

# Design Principles of CCN-AC

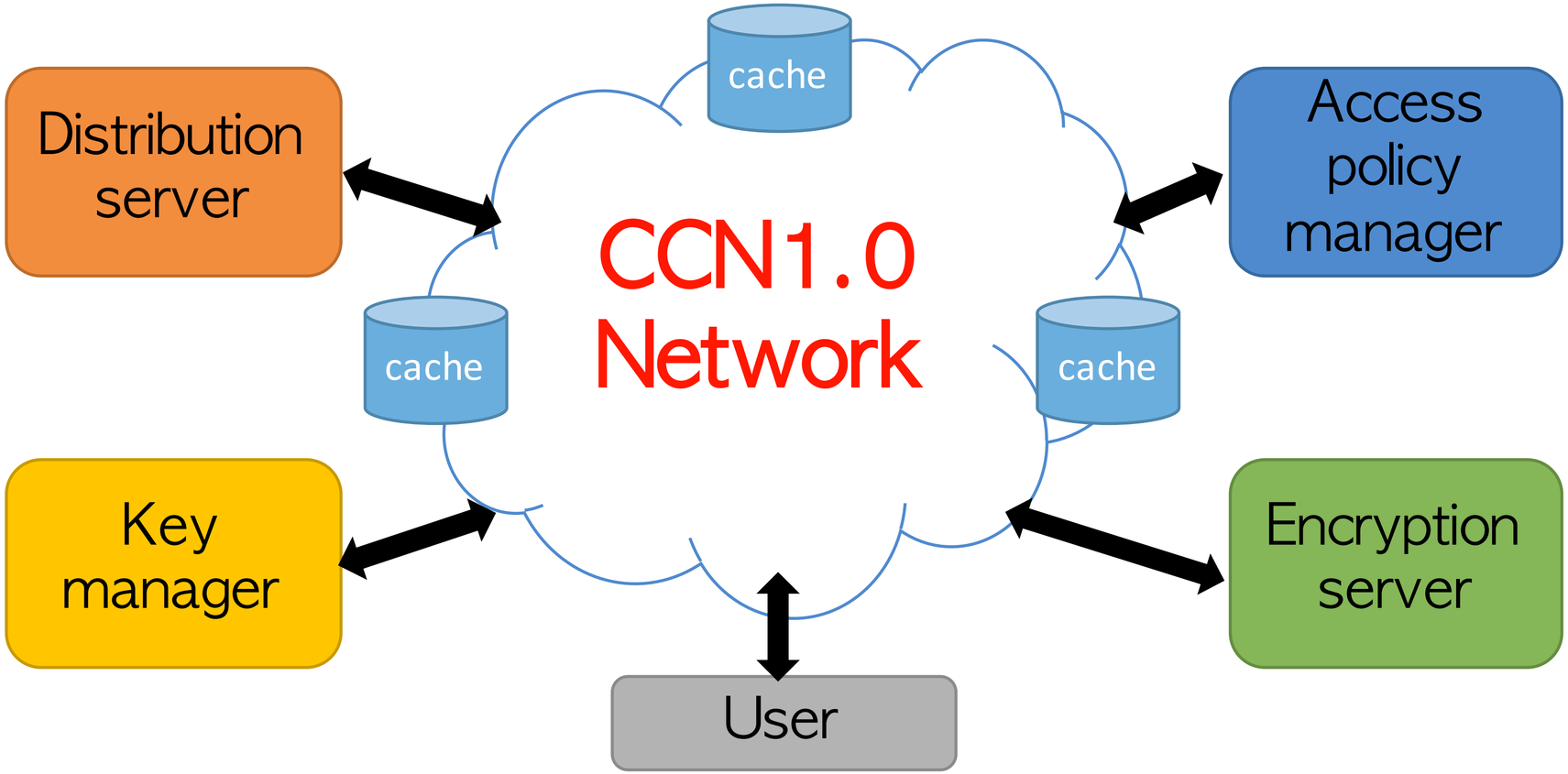
1. A **flexible and scalable framework** for encryption-based access control for CCN

   - **Flexible:** supporting different access control and encryption schemes

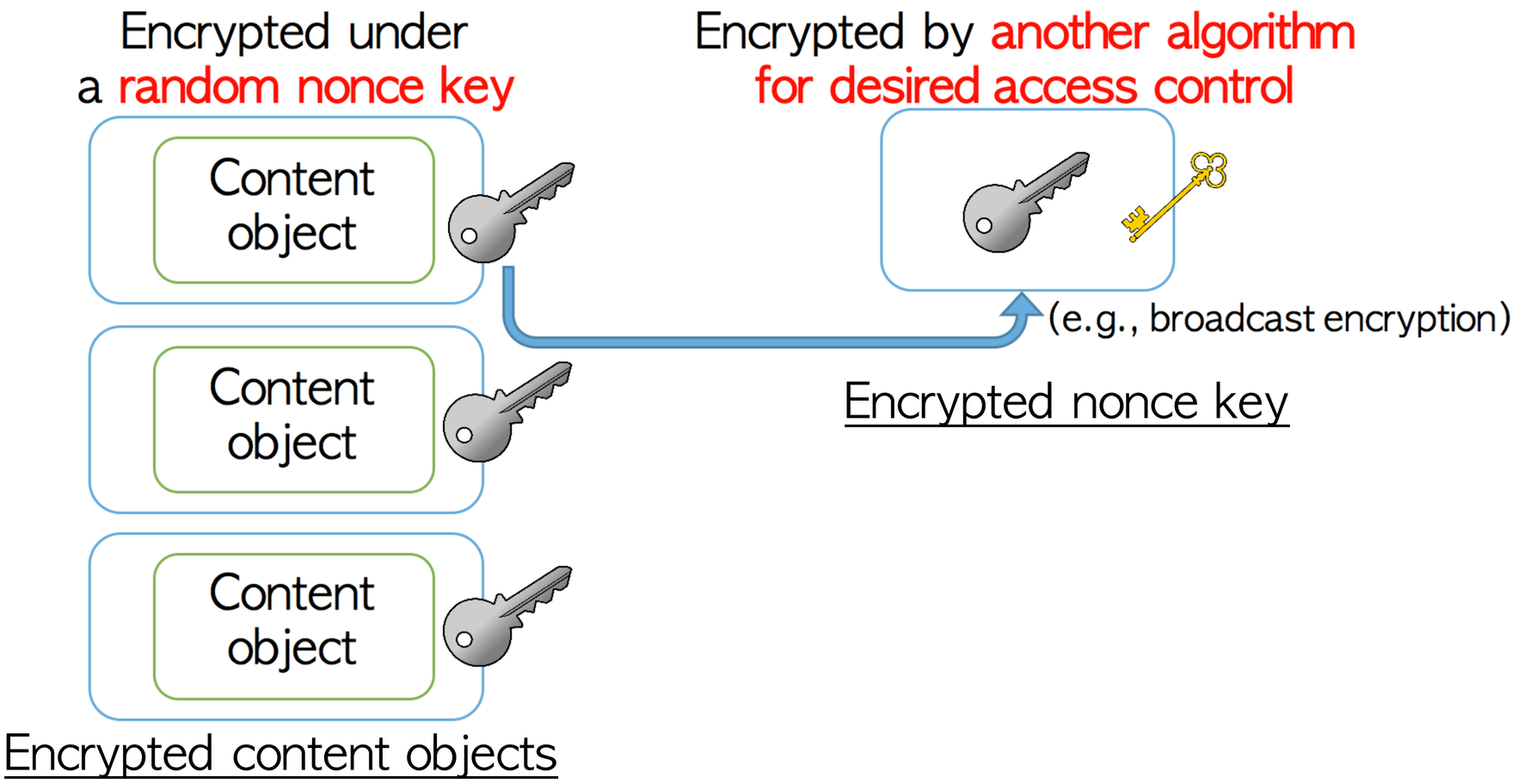
   - **Scalable:** accommodating large number of producers/consumers and distributed implementations

2. Maximize **cache utilization & usability**

# A Sample Distributed System



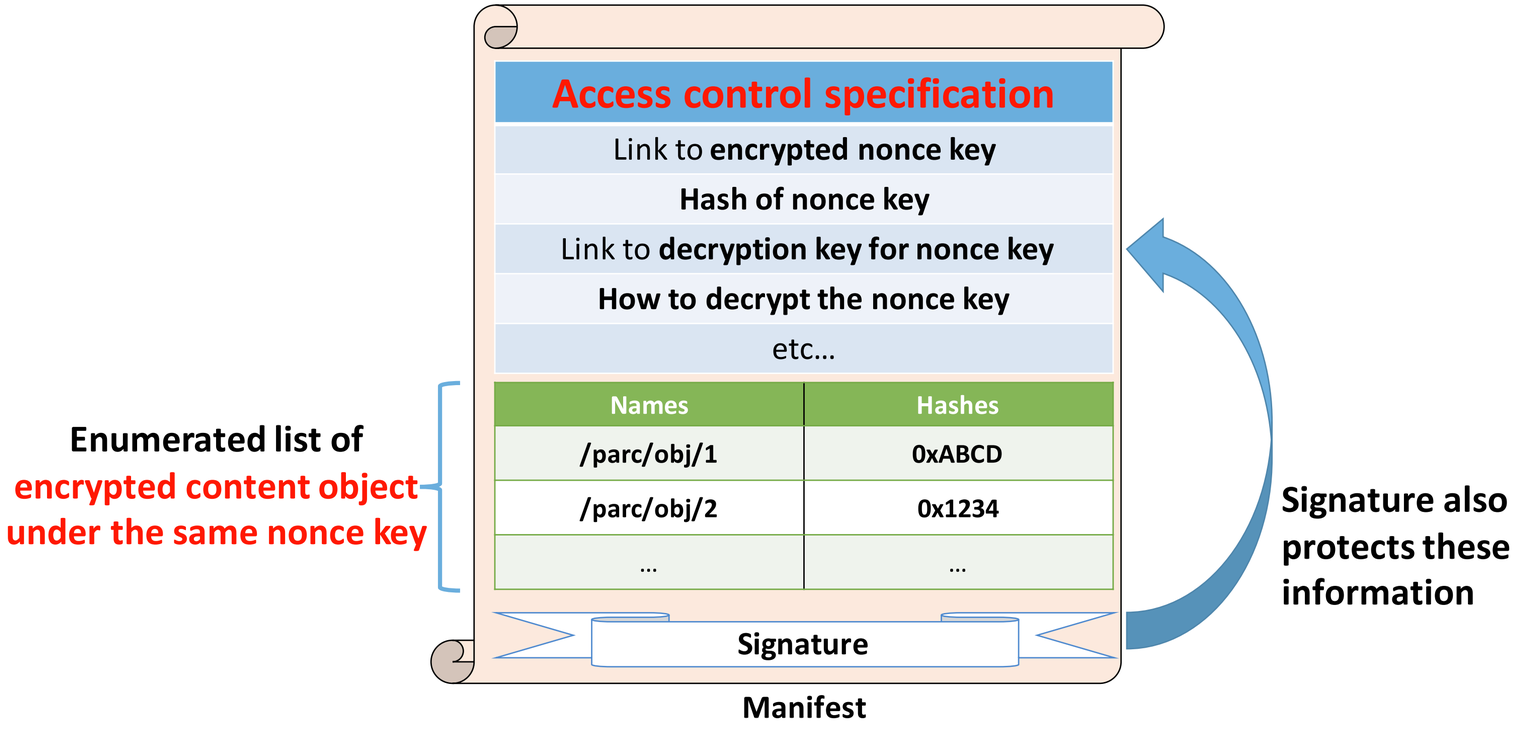
# Elements of CCN-AC (1): Hybrid Encryption



# Elements of CCN-AC (2): Manifests

Content Objects listed in a Manifest are encrypted under a random nonce key

All of the information needed to decrypt the listed content objects can be obtained **through the Manifest**



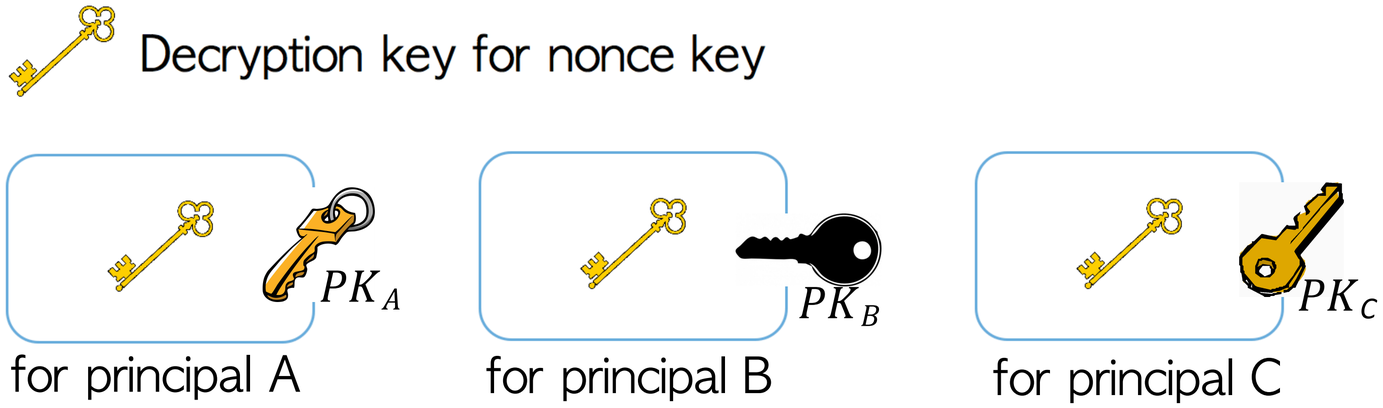



parc
A Xerox Company

# Elements of CCN-AC (3): Principal-Based Access

**Principal**: individual or group of users

Each principal i has a unique public/private key pair (PKi,SKi)

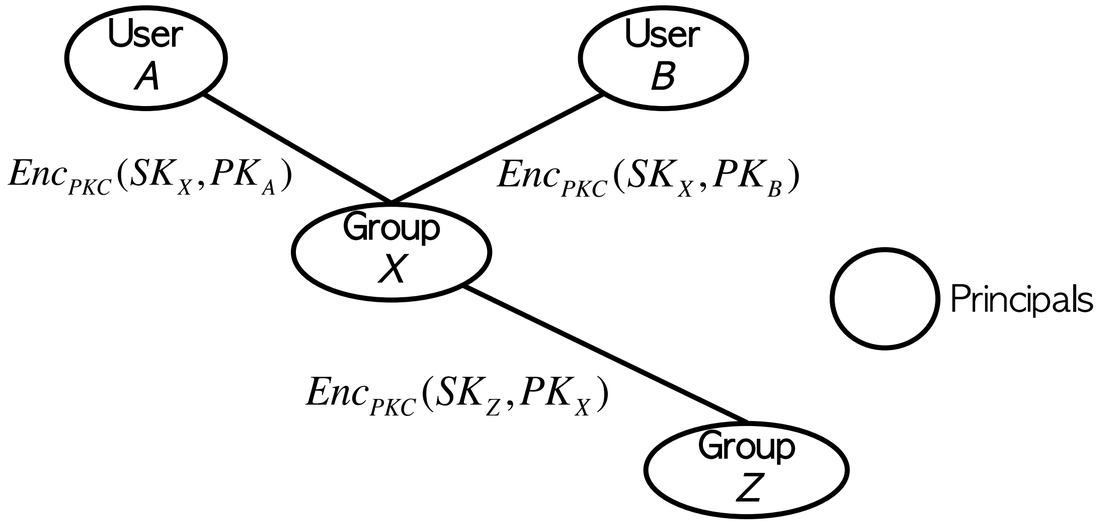


# Hierarchical Organization of Principals

Each principal's private key is encrypted with its children's public keys

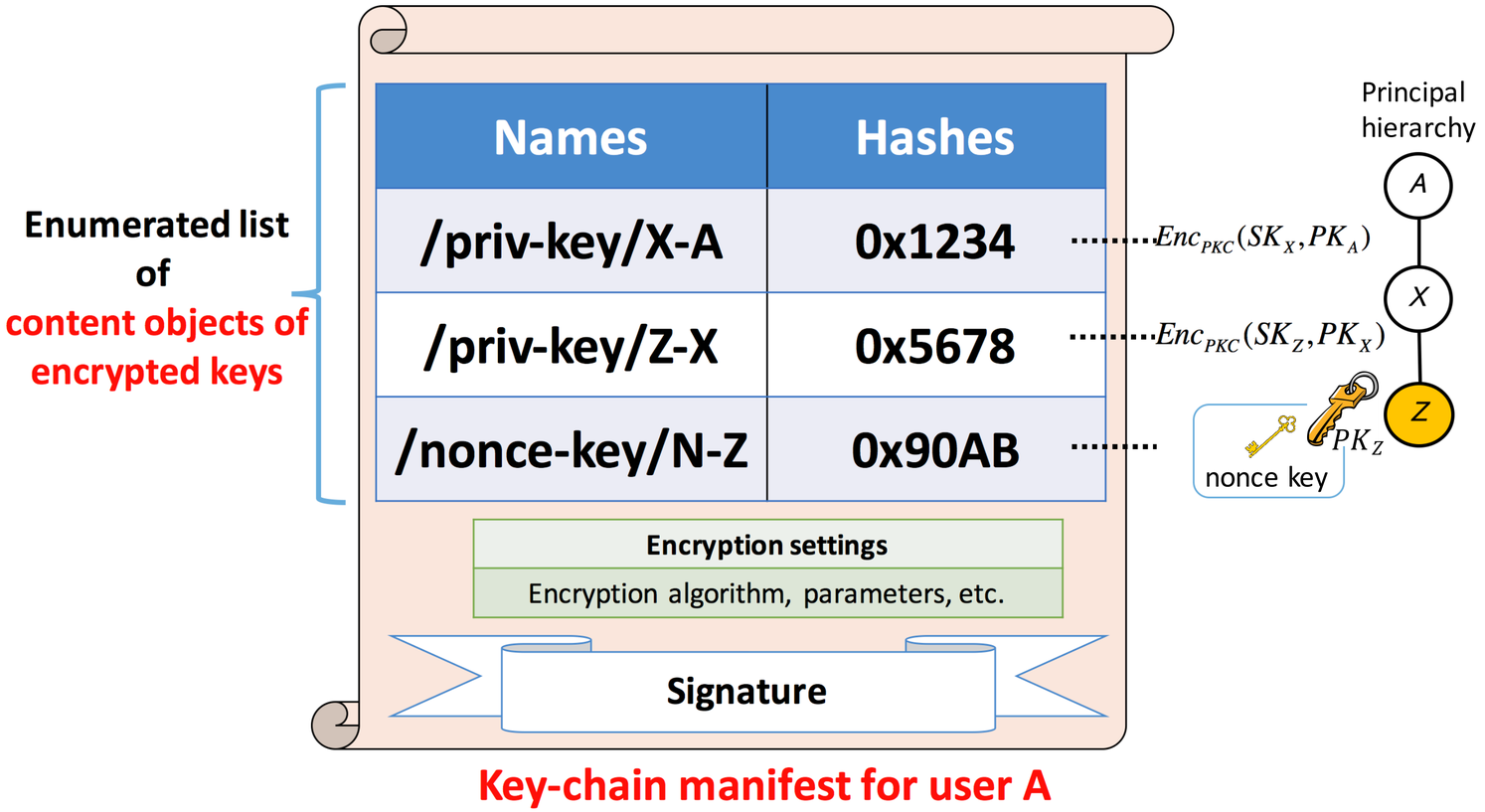
All encrypted keys are Content Objects

Only qualified users can disclose encrypted keys by traversing the principal hierarchy




Each principal's private key is encrypted its children's public keys

# Elements of CCN-AC (4): Key Chains



# Summary of CCN-AC Approach

1. **Hybrid encryption** of content objects

2. All access control information can be obtained from the **Manifest**

3. Access control is based around **principals**, which can be arranged hierarchically

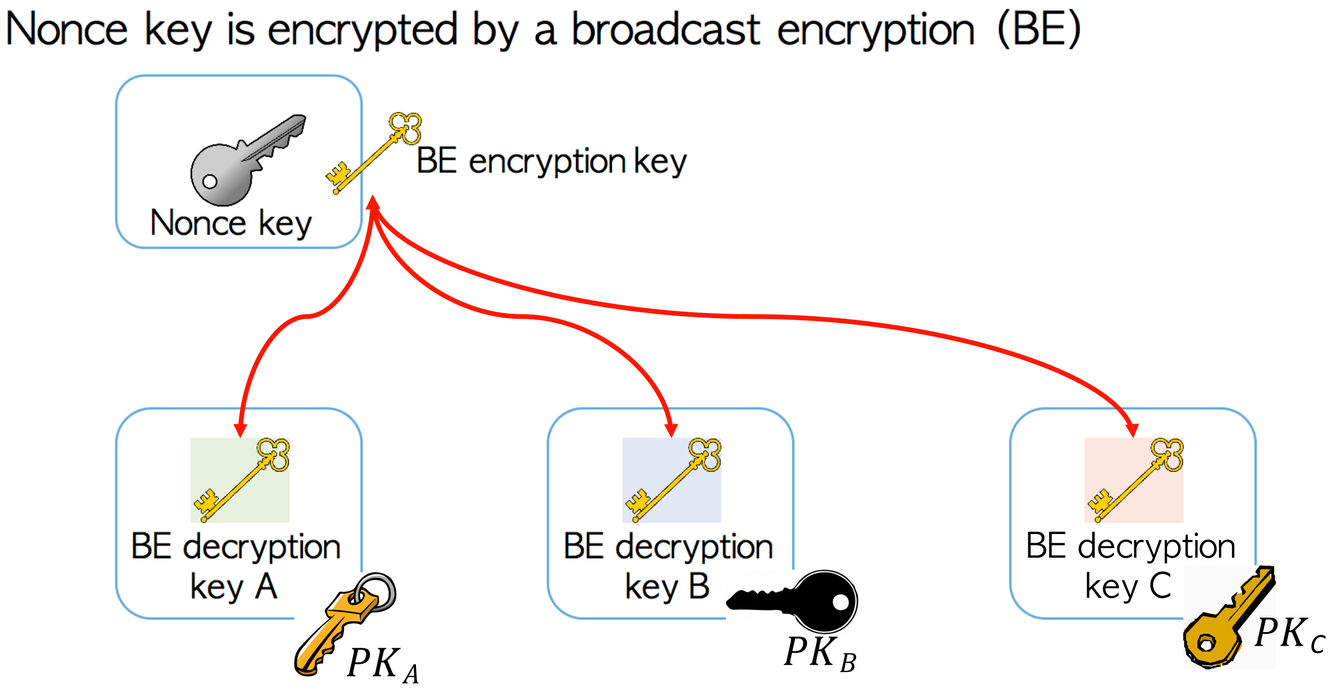
4. **Key chains** provide all of the keys necessary for qualified principals to recover the symmetric (nonce) key used to encrypt content

# Sample Instances of CCN-AC

# Broadcast-Encryption Based Access Control

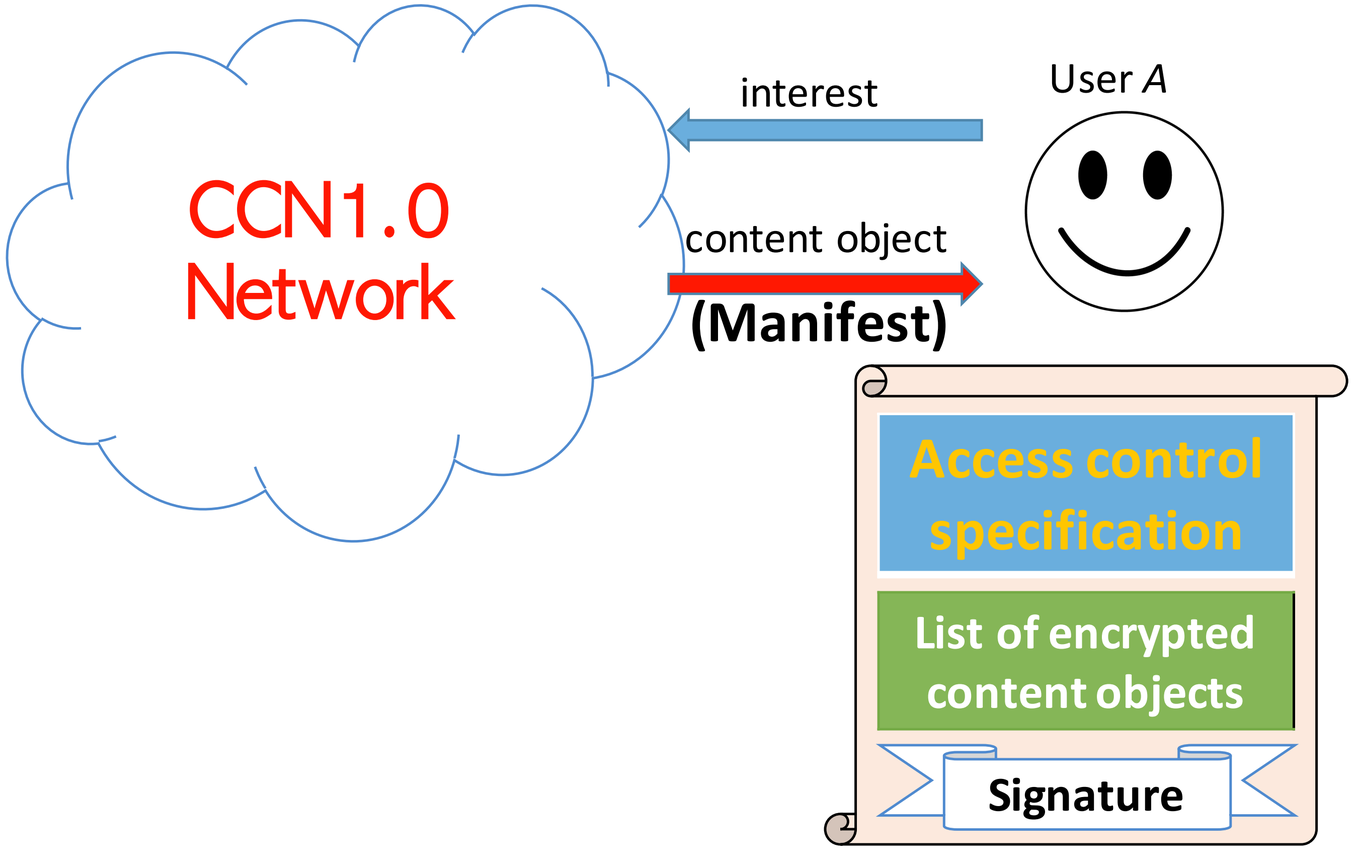
**Assumption:** individual principals are directly qualified to access content

**Setting:**



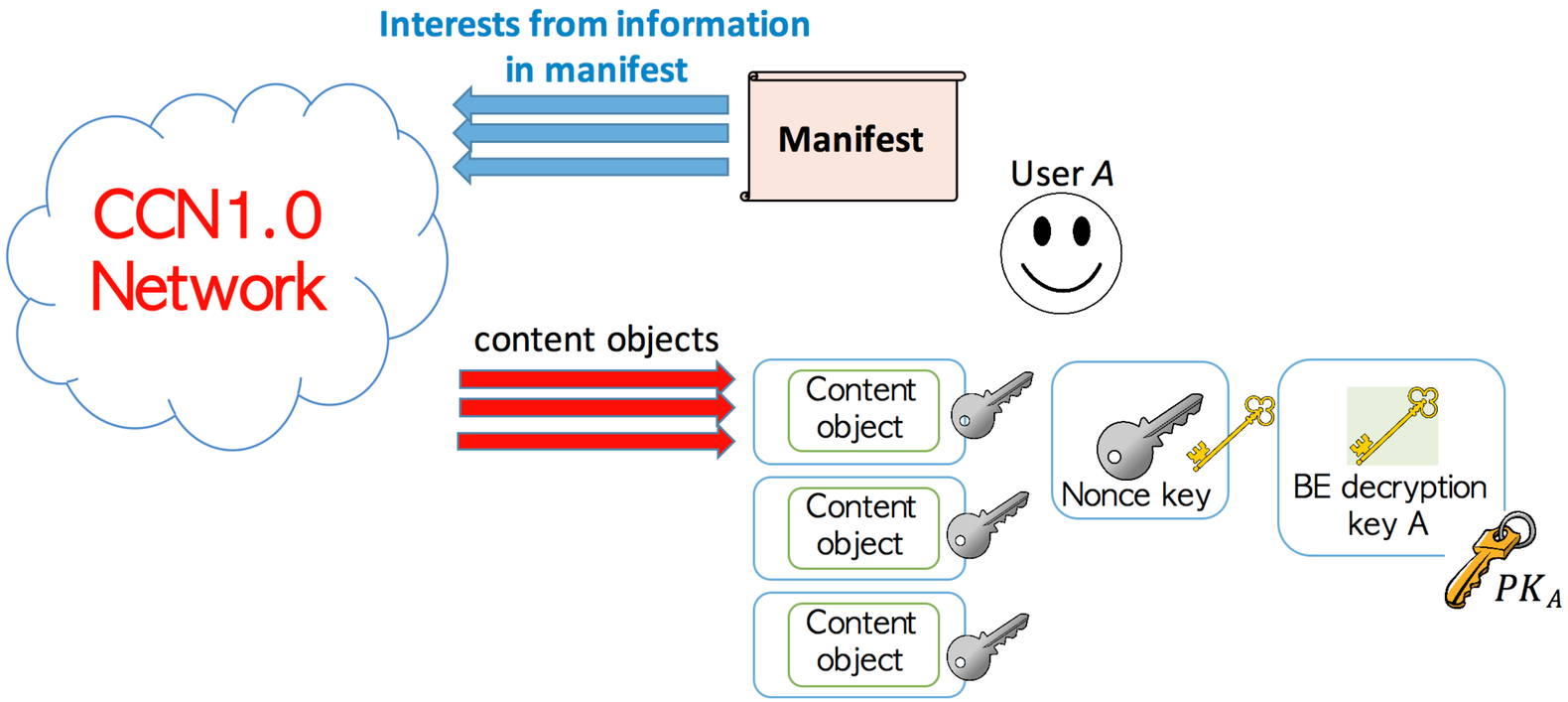
# Decryption Process (1)

Step 1)



# Decryption Process (2)

Step 2)






parc
A Xerox Company

# Other Instantiations

- Group-based access control

- Session (interactive) access control (e.g., TLS)

- Proxy (re-encryption) based access control

- Attribute-based access control

…

**For details and examples, please see our recent paper[1] and the technical report[2] :**

[1] J. Kurihara, E. Uzun, C. Wood, “An Encryption-Based Access Control Framework for Content-Centric Networking”, IFIP/IEEE Networking 2015

[2] J. Kurihara, E. Uzun, C. Wood, “CCN 1.0 Access Control Framework”, PARC Technical Report, May 2015

# Conclusions

CCN-AC:

- A flexible, scalable, and extensible AC framework for CCN

- Takes advantage of Manifests

- Designed to work with and take advantage of caching

# Questions?…

parc®

A Xerox Company

# Thank you