Towards Name-based Trust and Security for Content-centric Network

By:

Xinwen Zhang, Guangyu Shi, GQ Wang, Huawei R&D, Santa Clara, CA

Katharine Chang, University of Michigan, Ann Arbor, MI

Huijun Xiong, Virginia Tech, Blacksburg, VA

Yonggang Wen, Nanyang Technological University, Singapore

Motivations

- **Several Information Centric Network (ICN) architecture have been proposed for future Internet**
  - Content-centric network (CCN) / named-data network (NDN)
  - NetInf, PSIRP, DONA, …
- **Security is a built-in feature in ICN**
  - With the focus on content integrity and confidentiality
  - Trust is a pre-requisite for security
- **PKI-based trust management**
  - Not very scalable
    - S-BGP, soBGP, psBGP, SPV, …
  - Certificate distribution/management is complex
  - Deriving trust from key certificate is not efficient

Our Proposal

- **Name-based trust and security**
  - Leverage named content in network
- **Deriving trust from existing infrastructures**
  - Email, phone number, friend list, …
  - Leveraging social/admin/owner relationships, …
- **Identity-based signature (IBS) for content integrity verification**
  - Identities as public keys
    - Device id, content name/prefix, etc
  - Reduce the complexity of public key certificate management
- **Identity-based encryption (IBE) for content confidentiality**
  - Flexible secure data dissemination
    - No need to build a secure channel before content publish

IBC Algorithms

- **A trusted entity: private key generator (PKG)**
  - common trusted entity
  - but does not do certificate signing and key distribution
- **id: a public identity as a string**
  - Name, prefix, email, …

- **(pb, pr): a public/private key pair generated from id**

PKG:

Setup: 1^k -> SP, MSK, (PKG publishes SP, and saves MSK)
GeneratePrK: (id, MSK) -> pr_id

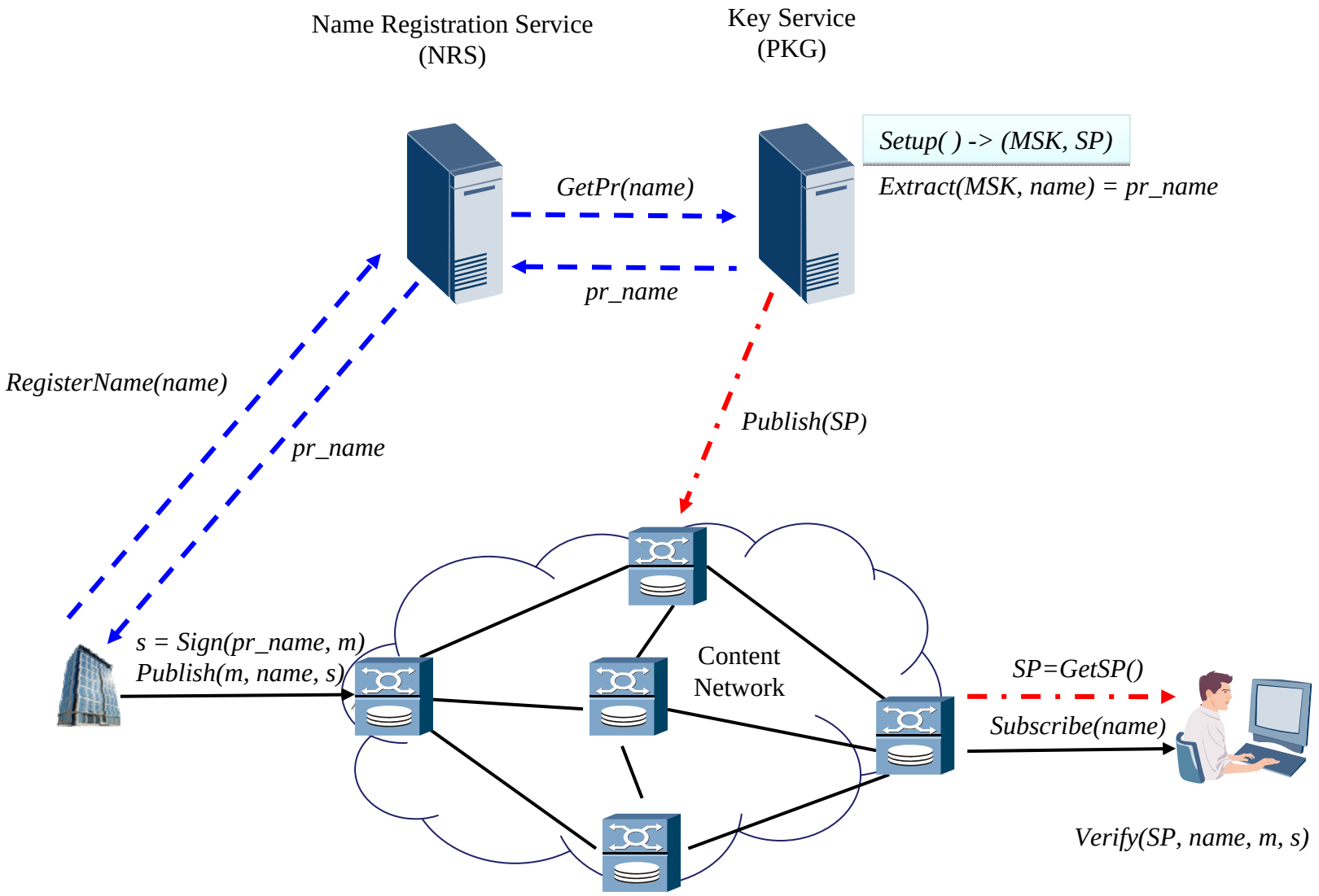
Sig:

Sign: (m, id, pr_id) -> s
Verify: (s, m, SP, id) -> true/false

Enc:

Enc: (m, id, SP) -> c
Dec: (c, pr_id) -> m

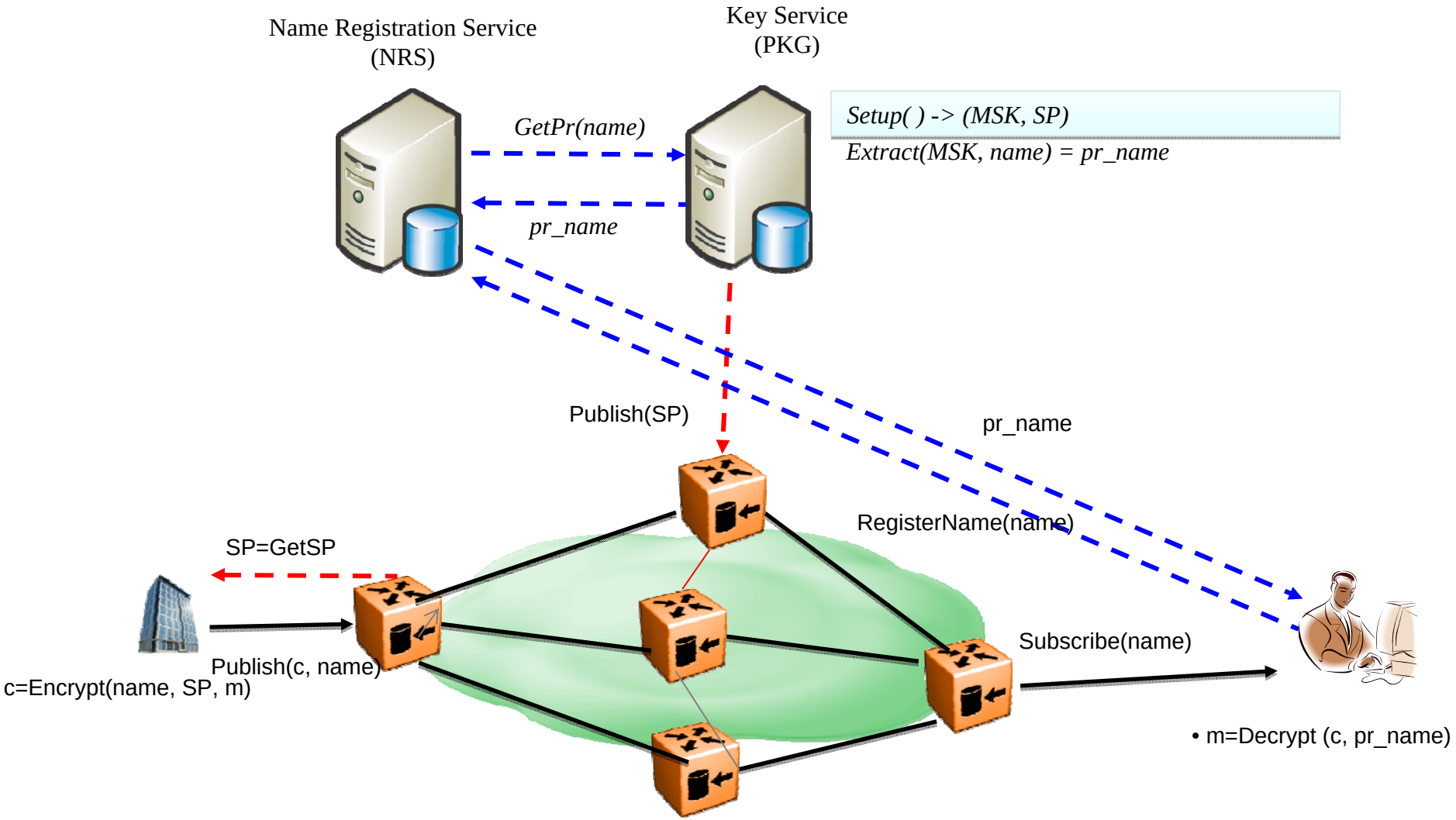
Name-based Signature for CON



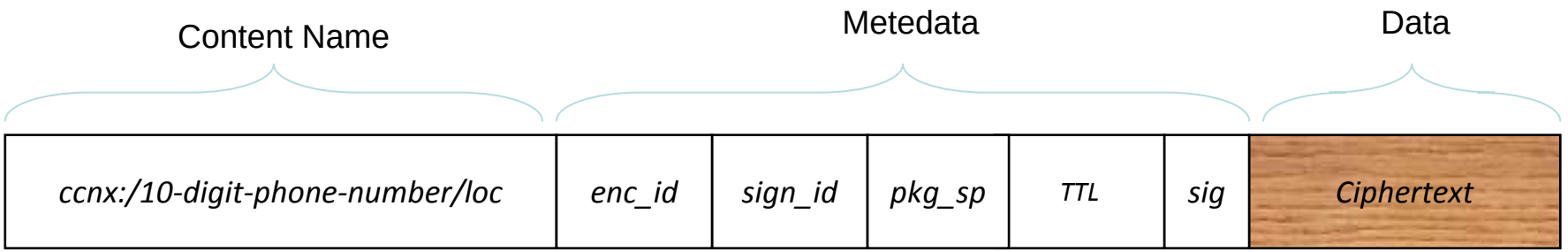
Secure Channel — Authenticated Channel — Data Transmission

HUAWEI

Name-based Encryption for CON



Data Format



- *enc_id:* the target name prefix that can decrypt
- *sign_id*: the name prefix that used for signature verification
- *pkg.sp:* the *SP* of the PKG (or its hash) corresponding the name prefix
- *sig*: signed hash of the content name, metadata, and ciphertext.

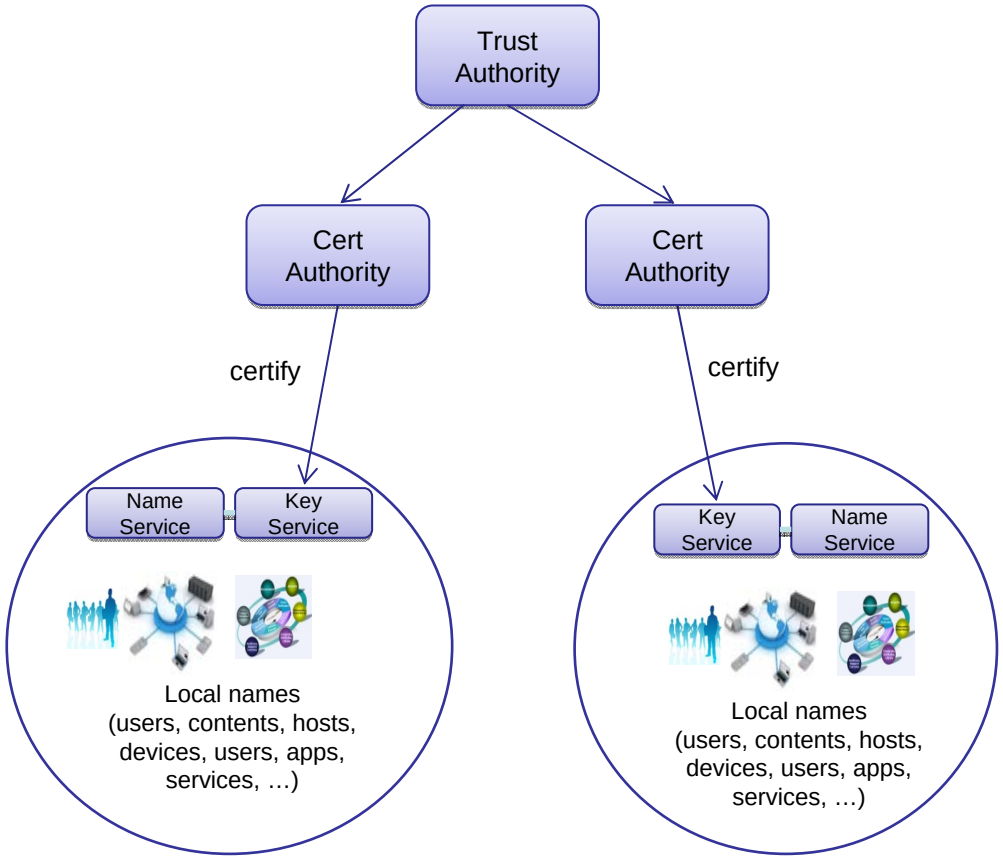
A Hybrid Scheme: PKI + IBC

- **Pure IBC is not scalable for Internet**
  - Centralized PKG is not scalable
  - Secure distribution of private key can be an issue
    - Should rely on some authentication mechanism
  - Authentication of PKG's SP can be an issue
    - May rely on another trust management infrastructure

- **Proposal: a hybrid trust management scheme: PKI + IBC**
  - PKG/NRS are domain/AS level services
  - Distribute private key within domain
    - Each organization can implement its own key distribution, with authentication mechanisms
    - For example, in an enterpise, username/passwrod, Kerberos, IAM (LDAP/Active Directory)

  - Distribute and verify SP with inter-domain PKI-based trust management
    - Domain level PKI is available actually:
      - DNSSEC, IPSec, SSL, RPKI, etc
    - A content publisher or consumer only needs to trust a few PKI-CAs

Hybrid Scheme: PKI + IBC



- PKG/NRS are within domain/AS level
- PKG issues private key for local names
- PKG.SP is certified by PKI CA

- certificate management complexity:
  - Pure PKI: O(nxm)
    - n - space of devices/users/hosts/services/names
    - m - space of domains
  - Hybrid: O(m)

IBC is good for user/app/device/host/service level trust and security
While PKI is good for domain/AS level

Discussion

- **Supporting flexible security policies:**
  - Group signing
  - Multiple signatures for single name
    - With different prefixes
  - Delegated signing

- **Self PKG**
  - Self-signed PKG.SP
  - Good for P2P, social network, and ad-hoc network

- **Private key revocation**
  - Private key is built with timestamp augmented id
    - Bob@huawei.com || Oct-2011

Implementation

- **CCNx-Latitude:**
  - A location sharing application on Android
  - Over CCNx project

Malicious CCNx client
• Sniff location data
• Publish fake location

Alice: Sender

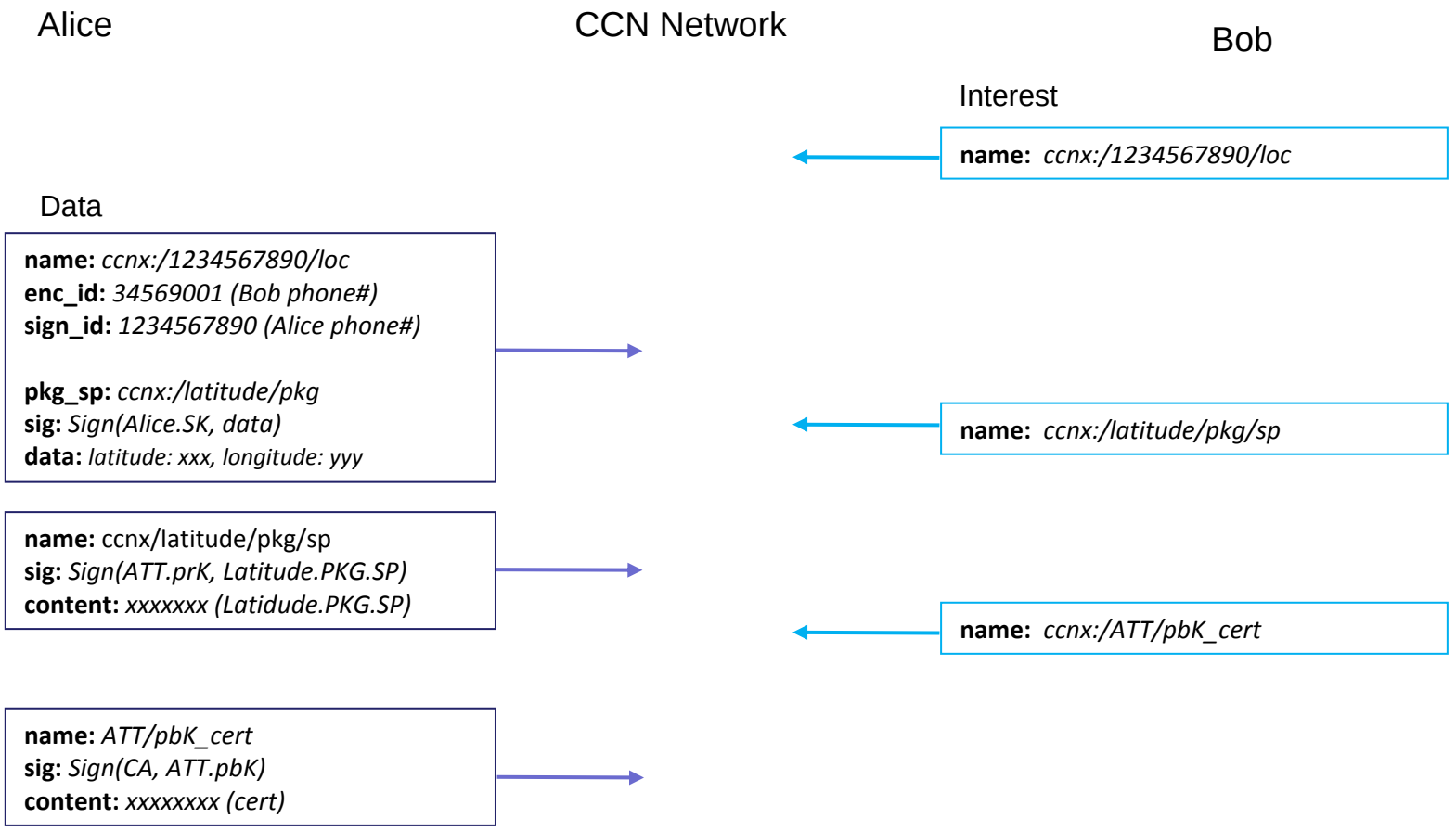
• React interests by generating content of location with name *ccnx:/phone-number/loc*
• Encrypted with receiver's *phone-number*
• Signed with sender's key
• Pre-loaded to device SD card

Bob: Receiver

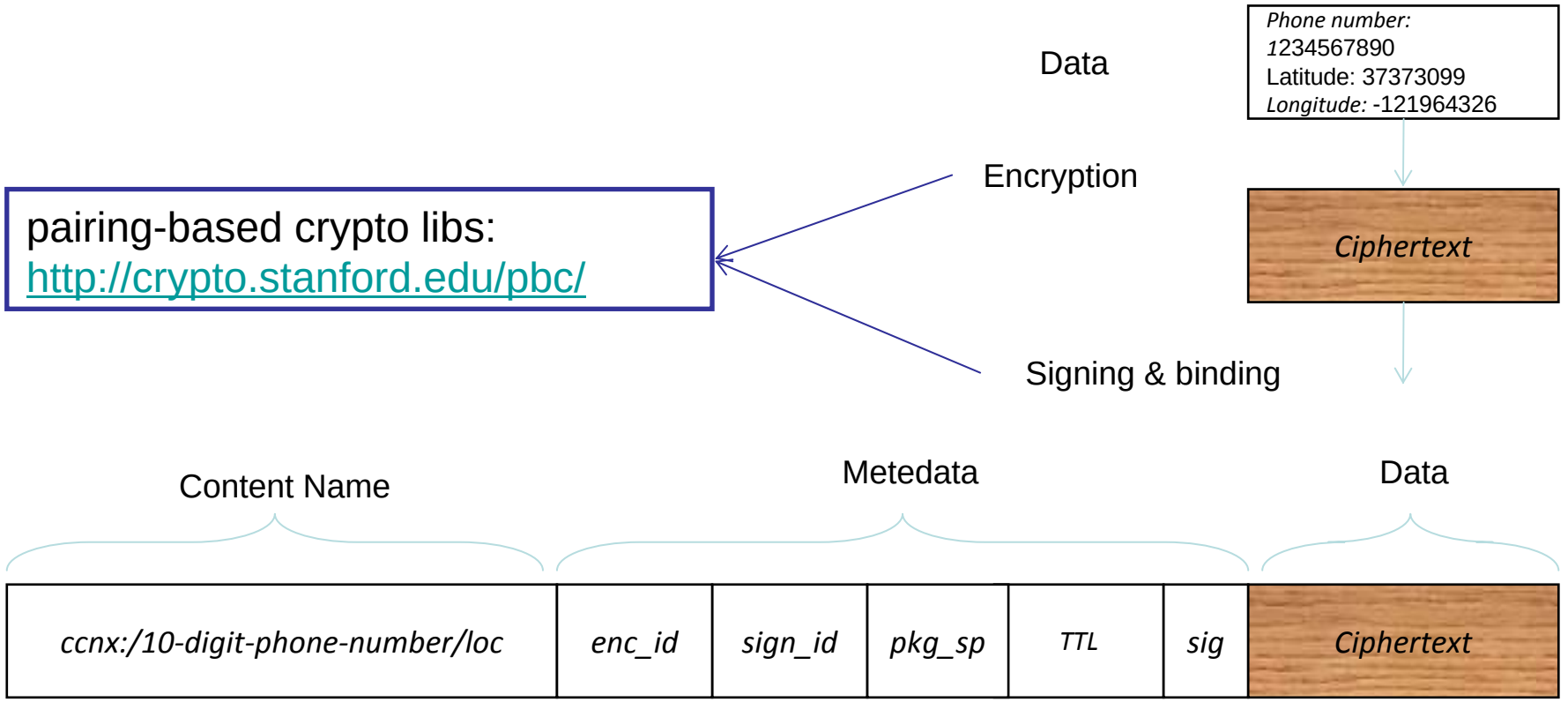
• Periodically send interest for *ccnx:/phone-number/loc*
• Sig verification and decryption
• Show location on map

HUAWEI

CCNx-Latitude Protocols



Content Name and Metadata



- *enc_id:* Bob's phone#
- *sign_id*: Alice's phone#
- *pkg.sp:* the *SP* of the PKG corresponding the identity
- *sig*: IBS(Alice's pr, ciphertext, Alice phone#)

Evaluation

- **Un-optimized implementation**
  - Android 2.3
  - Google Nexus S
  - Java BF-IPC implementation: http://crypto.stanford.edu/pbc/

- **BF-IBC is almost 10 times slower than RSA operations**
  - Due to expensive paring operation
  - But data size independent

- **Performance improvement**
  - key encapsulation mechanism
    - IBE work on an AES key
    - AES key is used for real data encryption
  - For 5MB data, the performance is < 3% more than RSA

Conclusion

- **We propose IBC for named content in ICN**
  - Name/prefix as public key
    - Good for CCN/NDN with user readable names
  - IBS for content integrity and authenticity verification
  - IBC for content encryption

- **We propose a hybrid trust management scheme**
  - IBC for intra-domain trust management
  - PKI for inter-domain trust management

- **We implement CCNx-Latitude for PoC:**
  - CCNx proejct
  - Secure and private location sharing with CCN

Ongoing and Future Work

- **Booting trust for group communication in ICN**
  - With hierarchical content names
- **Group-based security for data sharing with ICN**
  - Dynamic group memberships
  - Multicast encryption
- **Secure mobility in ICN**
  - Enabling virtual group in ICN
- **Secure routing in ICN**

QA: xinwen.zhang@huawei.com

THANKS!