Moderator-controlled Information Sharing by Identity-based Aggregate Signatures for Information Centric Networking

Tohru Asami[1], **Byambajav Namsraijav[1]**, Yoshihiko Kawahara[1], Kohei Sugiyama[2], Atsushi Tagami[2], Tomohiko Yagyu[3], Kenichi Nakamura[4], Toru Hasegawa[5]

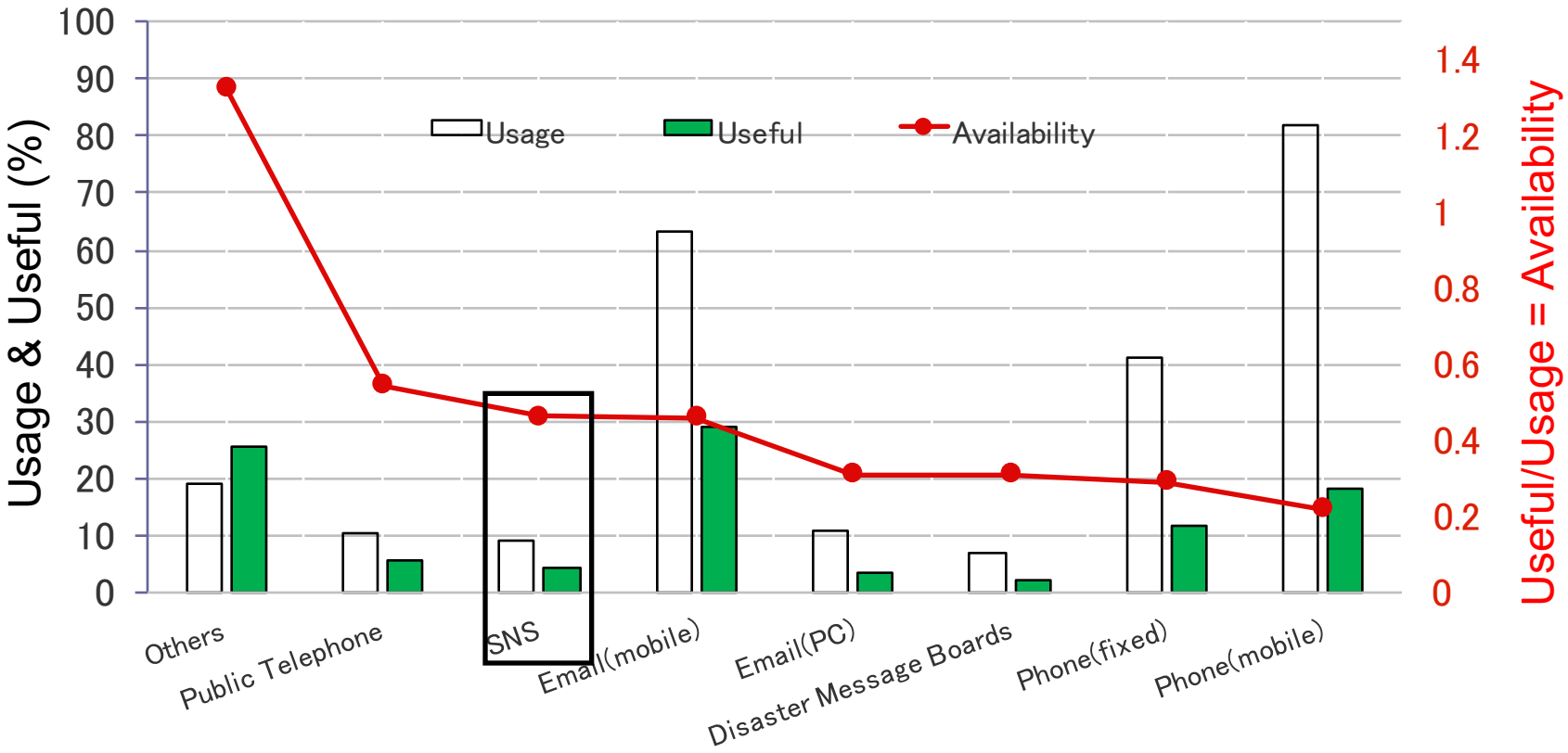
[1]The University of Tokyo
[2]KDDI R&D Laboratories
[3]NEC Corporation
[4]Panasonic Corporation
[5]Osaka University

Agenda

- Introduction
- Moderator Controlled Information-Sharing Service (MIS)
- Identity-Based Aggregate Signatures (IBAS)
- Implementation of IBAS in NDN
- Evaluation Results
  - RSA vs IBAS packet size comparison
  - Throughput (computational overhead)
- Conclusion
- Future Discussions

Introduction

Safety confirmation methods at the 2011 Tōhoku earthquake and tsunami



The availability of SNS was around 50%.
How to increase it?

Introduction

Goal

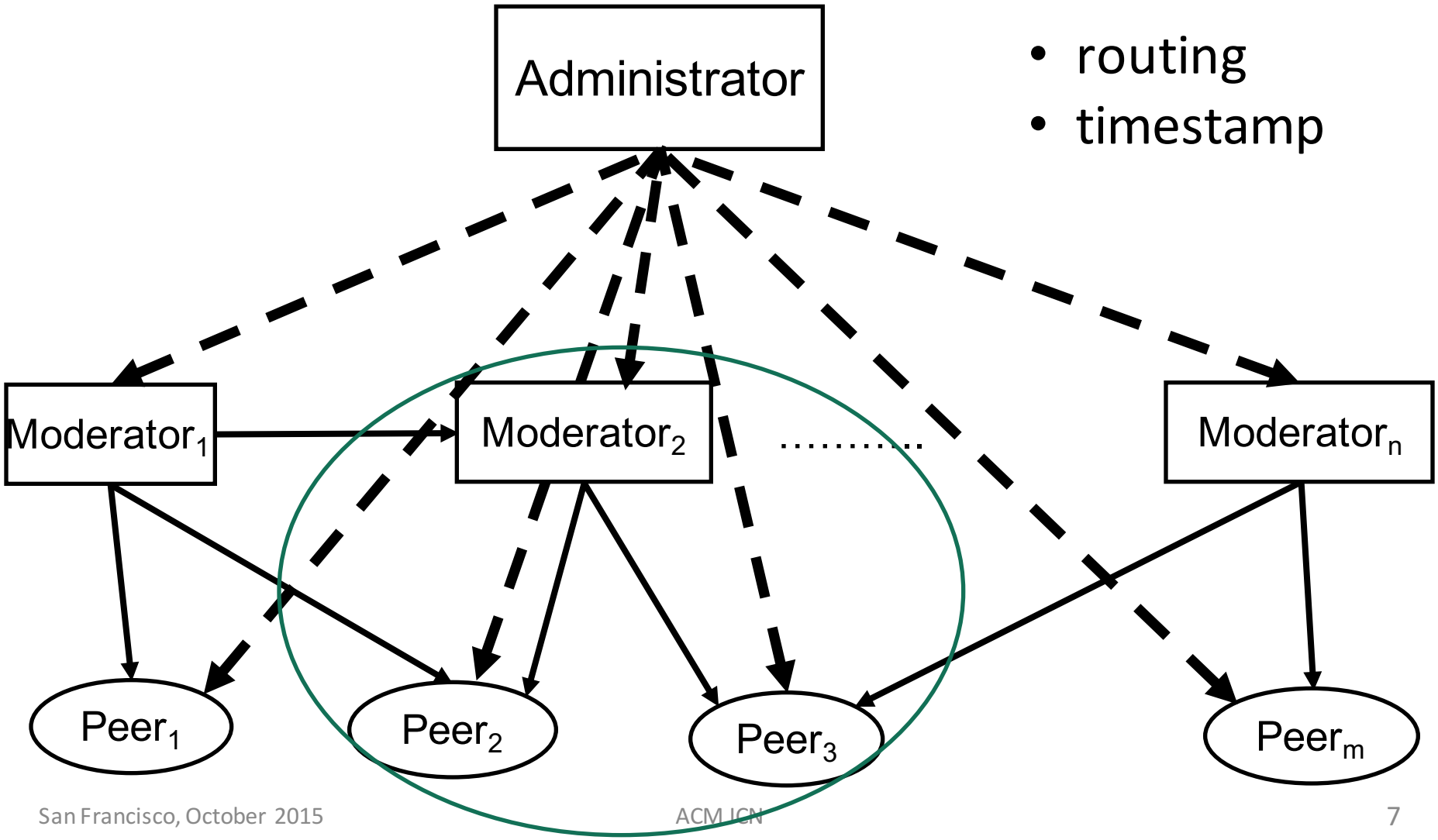
- All-weather social networking service (SNS)
  - Available even if the central server is down

Propose

- Moderator-controlled information sharing (MIS) service: an ICN-based distributed SNS

Moderator Controlled Information-Sharing Service (MIS)

Moderator Controlled Information-Sharing Service (MIS)

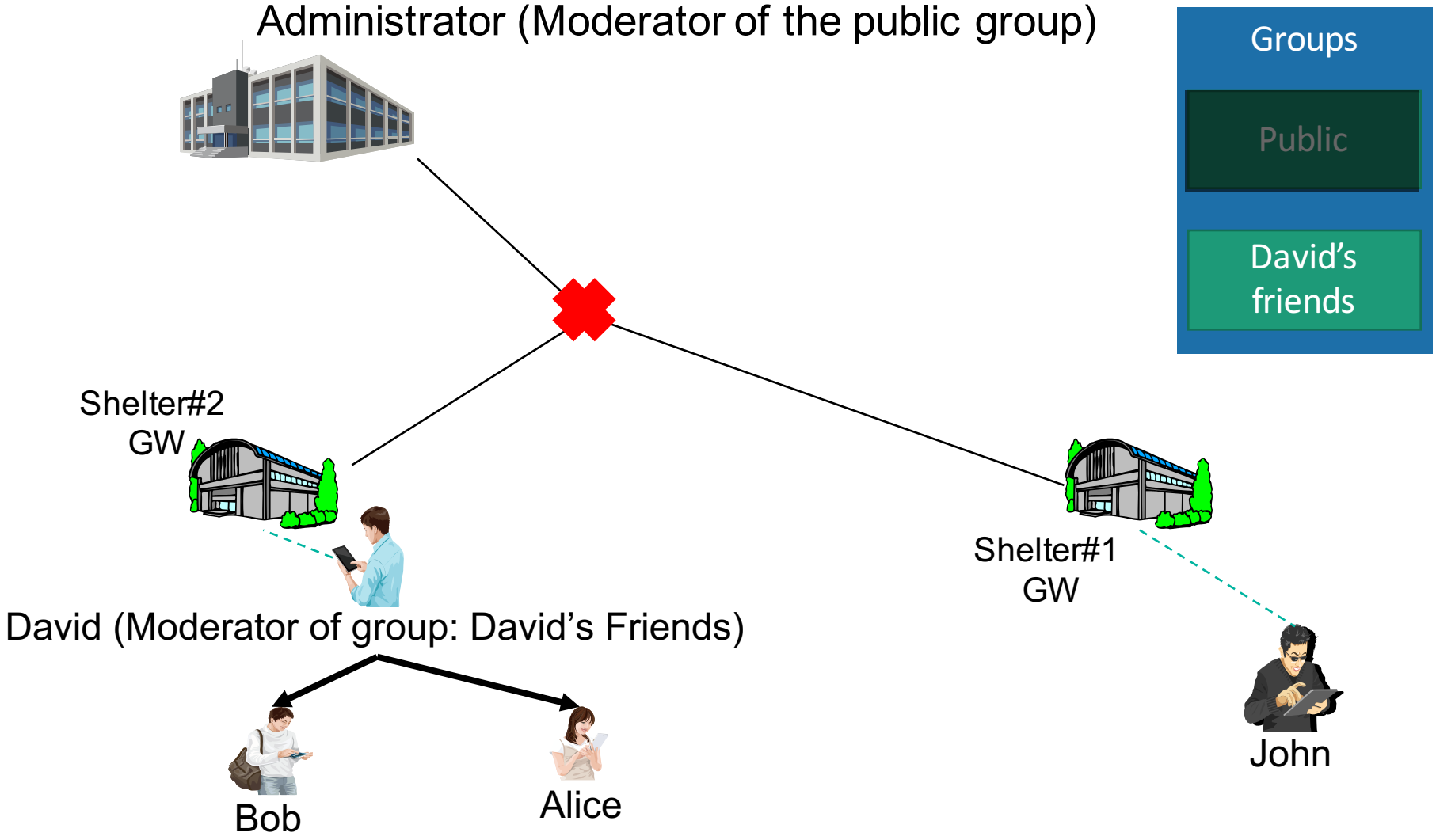


Roles of Entities

- Peer
  - publish messages to moderated groups
  - subscribe messages from moderated groups
- Moderator
  - check the messages in their group
  - timestamp the moderated messages
  - relay moderated messages to the peers
- Administrator
  - moderates the public group
  - conducts initial setups

to assure non-repudiation with signature

Moderator Controlled Information-Sharing Service (MIS) at a Disaster



Requirements for MIS (All-weather SNS)

Without relying on a central server:

- Peer can publish/subscribe a message if an accessible moderator exists
- Subscriber can verify the publisher and moderator's authenticity
- Assure non-repudiation

Advantages of ICN for MIS

Content signatures

- **authentication** of received messages

Network caches and routing

- **Fault tolerant** even if the administrator is unreachable

Disadvantages of ICN for MIS

Central verification authority of public key infrastructure (PKI) must be reachable

- In a disaster scenario, one may not be able to verify a message's signature if a required Certification Authority (CA) is out of reach.

Solved by ID-based Signatures

Large overhead for short messages

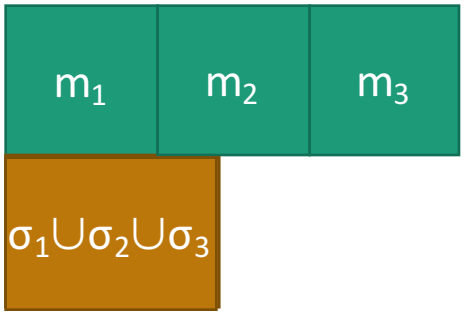
- Each message contains two signatures

Solved by Aggregate Signatures

Identity-Based Aggregate Signatures (IBAS)

Aggregate signatures and Identity-based signatures

- **Aggregate signatures** : aggregating *n* signatures on *n* distinct messages from *n* distinct users into a single signature of constant size



- **Identity-based signatures**: IDs such as email address or phone number is used instead of public keys. Verifier only needs PKG's public parameter and the signer's ID to verify a message.

Propose ICN with Identity-based Aggregate Signatures (IBAS)

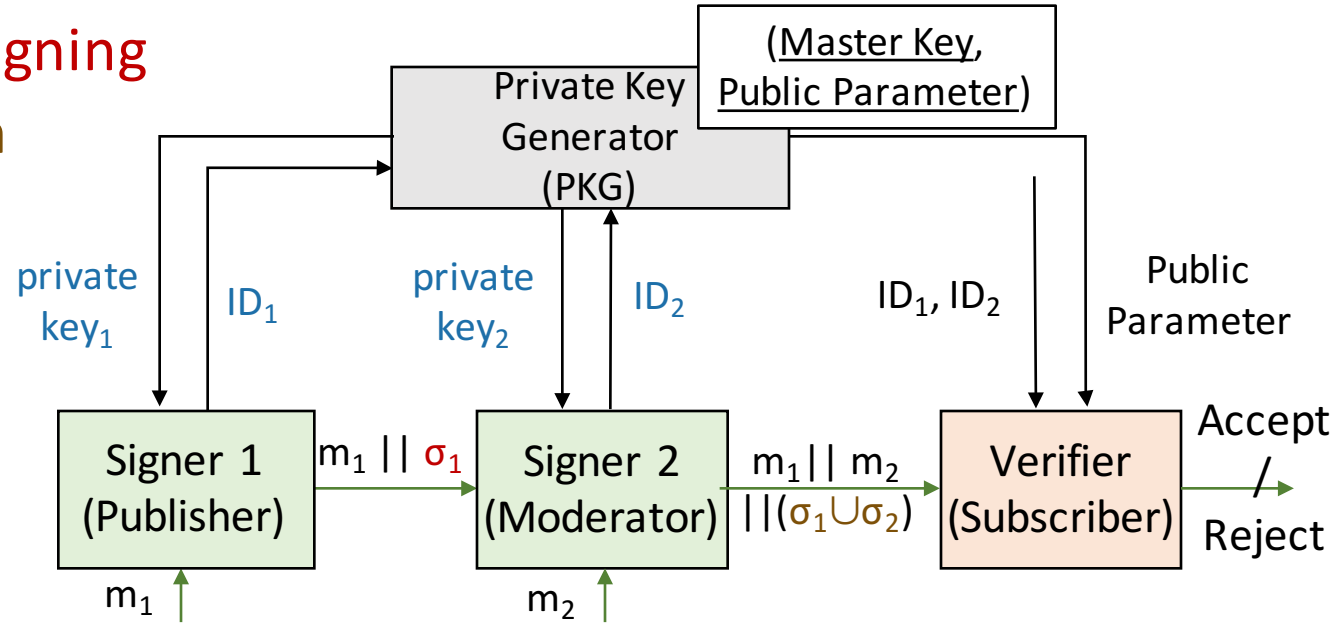
IBAS [1]: combination of aggregate signatures and IBS

IBAS operations

- Setup
- Private key distribution
- Individual signing
- Aggregation
- Verification

Offline

Online



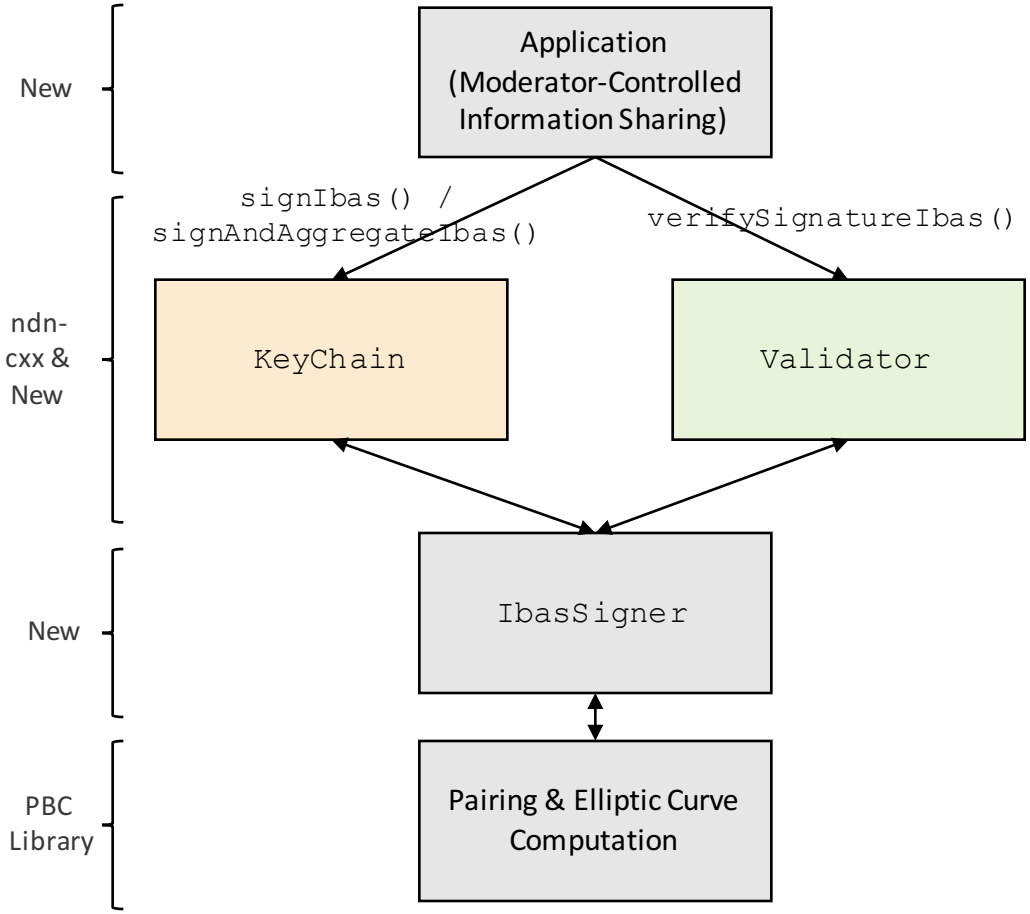
[1] Gentry, Craig, and Zulfikar Ramzan. "Identity-based aggregate signatures."

Implementation of IBAS in NDN

Implementation of IBAS in NDN[1]

Extend NDN's open source C++ library ndn-cxx [2].

- Add a new `SignatureType` named *SignatureSha256Ibas* which tells that the content is signed using IBAS.
- Use PBC Library[3] for pairing and other elliptic curve computations.



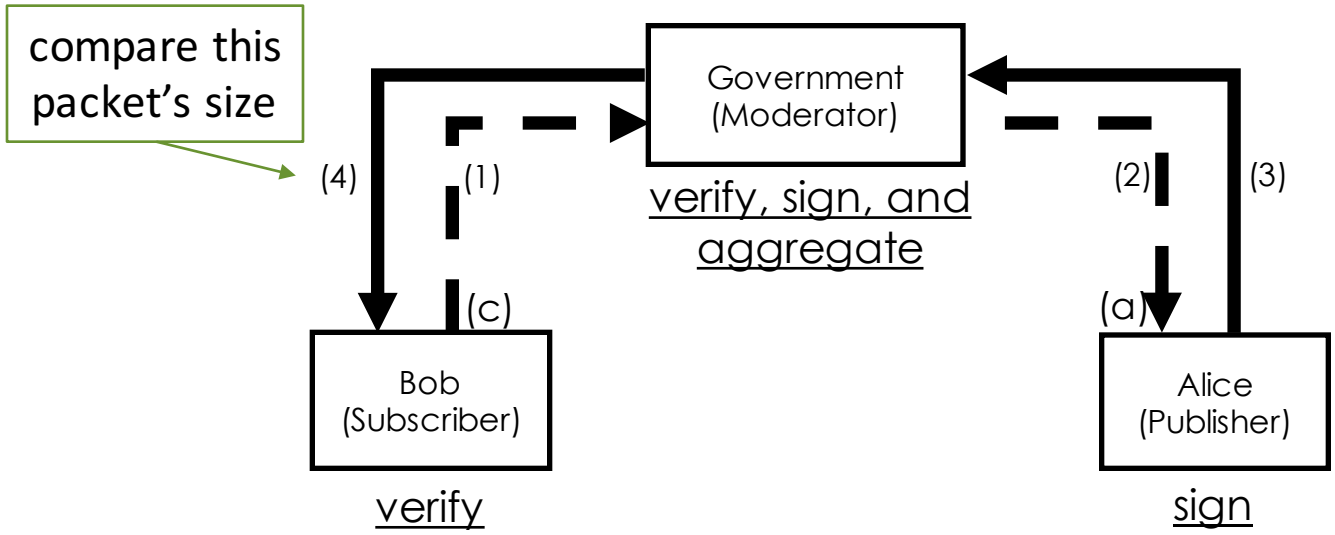
[1] https://github.com/byambajav/ndn-ibas
[2] https://github.com/named-data/ndn-cxx
[3] https://crypto.stanford.edu/pbc/

Evaluation Results

Evaluation Scenario

Measure following two metrics

- **Signature size**: for a disaster scenario
- **Computational overhead** of signature generation and verification: for normal condition

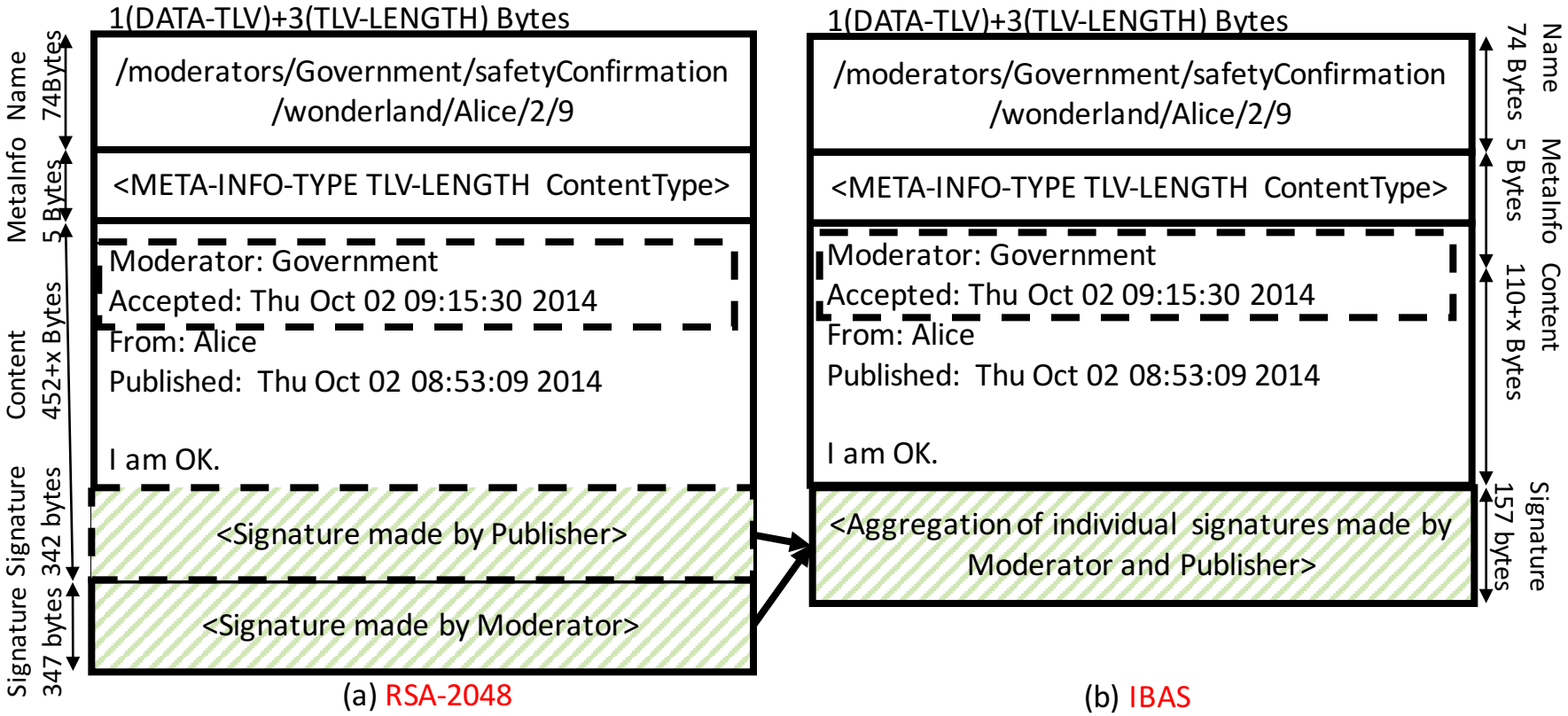


Evaluation Scenario: Assumptions

- IBAS's offline steps (*setup* and *private key distribution*) are done beforehand.
- In PKI, the subscriber has all the certificates required for signature verification in advance.

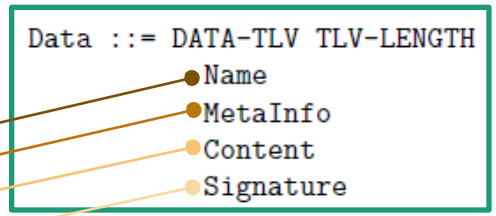
Results: RSA vs IBAS packet size comparison

Structure of a data packet sent from moderator to subscriber



Results: Message size reduced by 60%

Packet size* of different signature methods (byte)



a: Publisher to Moderator

	TLV	N.	M.I.	Con.	Sig.	Total
RSA-2048	4	46	5	$53+x$	$82+260$	$450+x$
RSA-1024	4	46	5	$53+x$	$82+132$	$322+x$
ECDSA-521	4	46	5	$53+x$	$82+126$	$314+x$
IBAS(512, 160)	4	46	5	$53+x$	$5+152$	$265+x$

b: Moderator to Subscriber

message content size

	TLV	N.	M.I.	Con.	Sig.	Total
RSA-2048	4	74	5	$452+x$	$87+260$	$882+x$
RSA-1024	4	74	5	$324+x$	$87+132$	$626+x$
ECDSA-521	4	74	5	$318+x$	$87+126$	$614+x$
IBAS(512, 160)	4	74	5	$110+x$	$5+152$	$350+x$

Thus, in case of a message "*I'm OK*" (6 bytes) the size of the packet sent from moderator to subscriber will be 888B and 356B for RSA-2048 and IBAS respectively

*size also depends on the participators' names

Results: Assumptions of computational overhead comparison

- Choose signatures of almost same strength: RSA-2048, ECDSA-256, and IBAS(224, 112)

qbits rbits

Comparable Strengths

IFC (e.g., RSA) and ECC (e.g., ECDSA)

RSA	ECC Type 1 [1] (NIST 800-57)	ECC Type 1 [2] (M. Yasuda et al.)
1024	160-223	133
2048	224-255	195
2671		224
3072	256-383	
3241		247
7680	384-511	
15360	512+	

[1] NIST, "Recommendation for Key Management"

[2] Yasuda et al, "On the strength comparison of the ECDLP and the IFP "

Evaluation environment

- OS: Ubuntu 14.04
- Hardware specifications
  - Model name: Intel(R) Core(TM) i7-3520M
  - CPU frequency: 2.9GHz
  - Cache size: 4MB

Results: Computational overhead is 2.4 times bigger than that of RSA

Signature processing times (ms)

	Publisher Alice	Moderator Government	Subscriber Bob
IBAS(512,160)	7.53	21.5	21.5
IBAS(224,112)	2.46	4.95	4.10
ECDSA-384	2.15	7.04	5.38
ECDSA-256	1.05	4.33	2.55
RSA-4096	10.2	10.4	0.446
RSA-2048	2.08	2.04	0.307
RSA-1024	0.738	0.841	0.246

IBAS(224, 112)
≈ ECDSA-256
≈ 2.4 x RSA-2048

Video communication: IBAS(224, 112) can achieve throughput of 2.4Mbps when each packet's content size is 1497bytes (IEEE802.3).

Conclusion & Future Discussions

Conclusion

- All-weather SNS: **Moderator Controlled Information-Sharing Service (MIS)**
- Core technology of MIS is Identity-based Aggregate Signatures (IBAS)
- Implementation on NDN is evaluated against the traditional PKI signatures.
  - 60% smaller packet size:
    suitable for usages at a disaster
  - 2.4 times larger computational overhead:
    2.4Mbps throughput on Intel i7-3520M@2.9GHz in normal condition

Future Discussions

- IBAS key parameter size choice
- Distribution of secret parameters and key revocation
- Improve current implementation toward a testbed experiment as a real world application

Thank you for your attention

Q&A

Acknowledgements

Parts of this research was funded by the joint EU FP7/NICT GreenICN project, under EU grant agreement 608518 and NICT contract 167.