CIS 700/002 : Special Topics : Secure MQTT for IoT

Sangdon Park

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania

March 30, 2017

Penn Engineering

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

What is MQTT?

- Message Queue Telemetry Transport (MQTT) is a publish-subscribe-based "lightweight" messaging protocol over TCP/IP protocol

TABLE I: MQTT Header

bit	7	6	5	4	3	2	1	0
byte 1	Message Type				DUP Flag	QoS Level		Ret
byte 2	Remaining Length							
Variable Header								
Payload								

https://en.wikipedia.org/wiki/MQTT

Why MQTT?

- Quite popular
  - Facebook Messenger
  - AWS IoT
- Lightweight
  - Minimize code footprint on devices
  - Reduce network bandwidth usages

The goal of “Secure” MQTT

- Authenticate each IoT device
- Encrypt communication channels btw IoT devices
  - Focus of this paper

“Secure” MQTT Alternatives

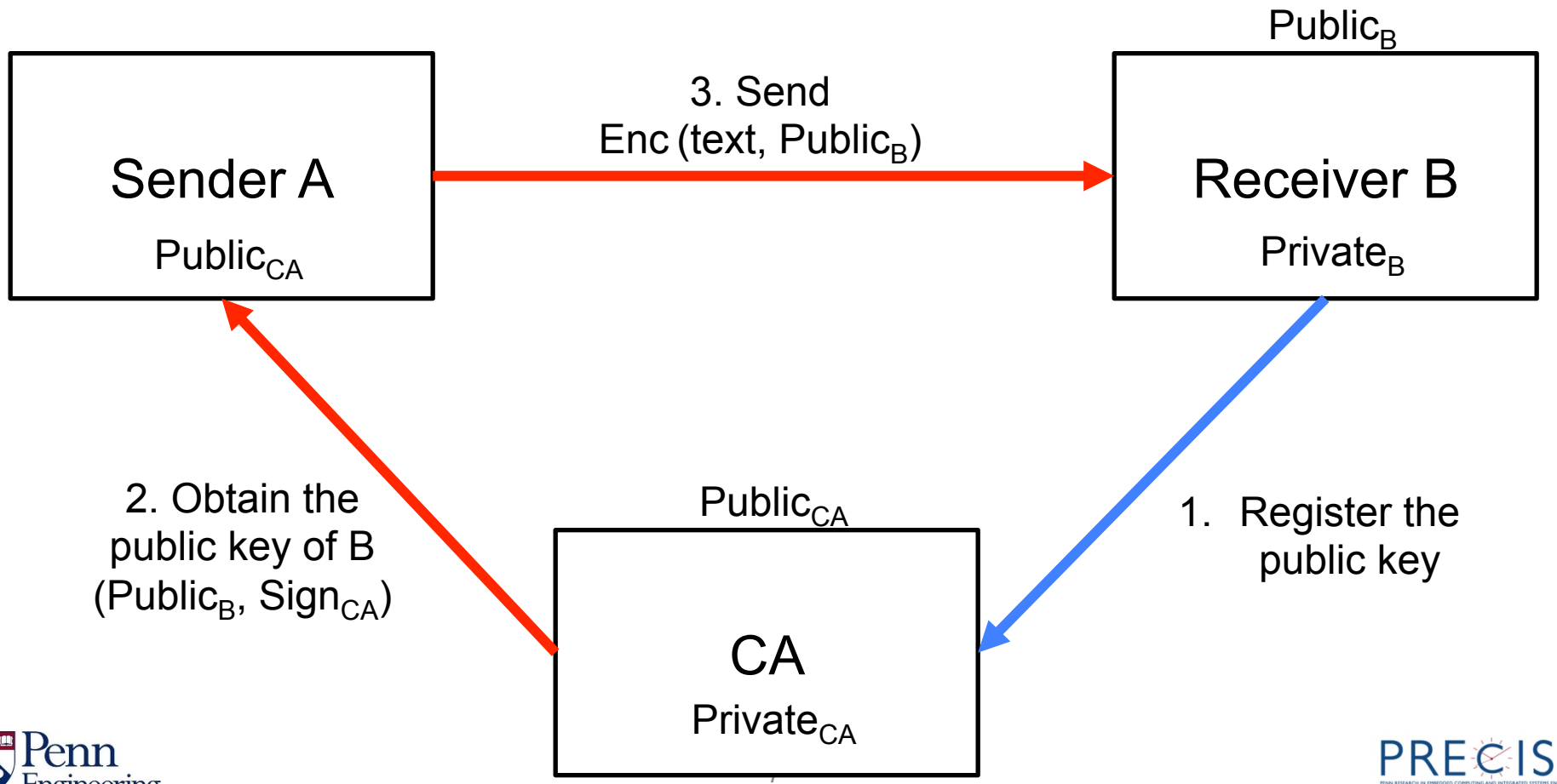
- MQTT + SSL/TLS
  - Storing and managing the certificates are cumbersome
  - SSL/TLS is weak on various attacks (e.g., BEAST, CRIME, RC4, Heartbleed)
  - (we think) key revocation is not simple

Contributions

- Proposes a secure MQTT protocol
  - MQTT + Attribute Based Encryption (ABE)

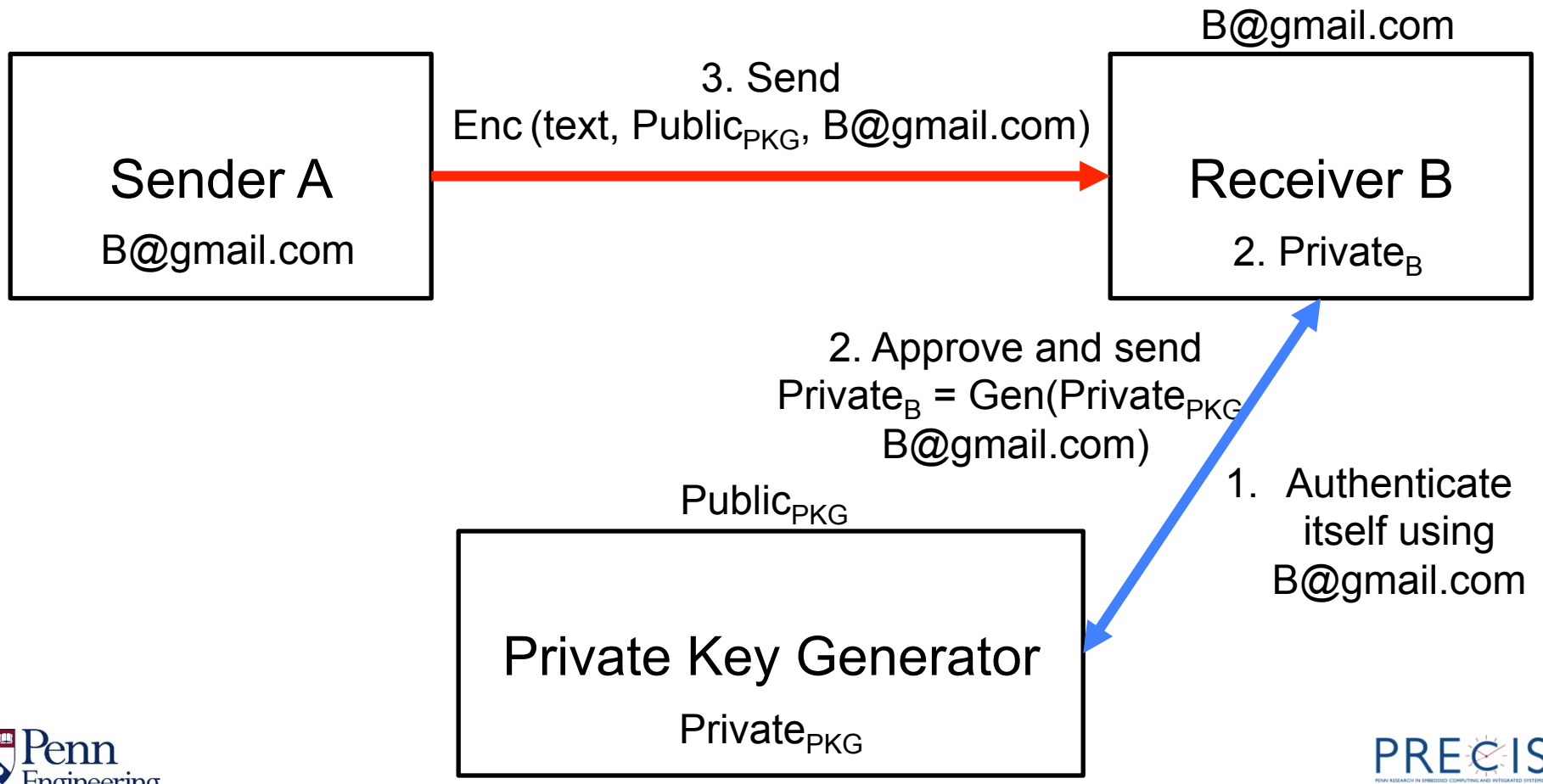
Public-key Encryption

- Identity of a receiver
  - The public key of the receiver



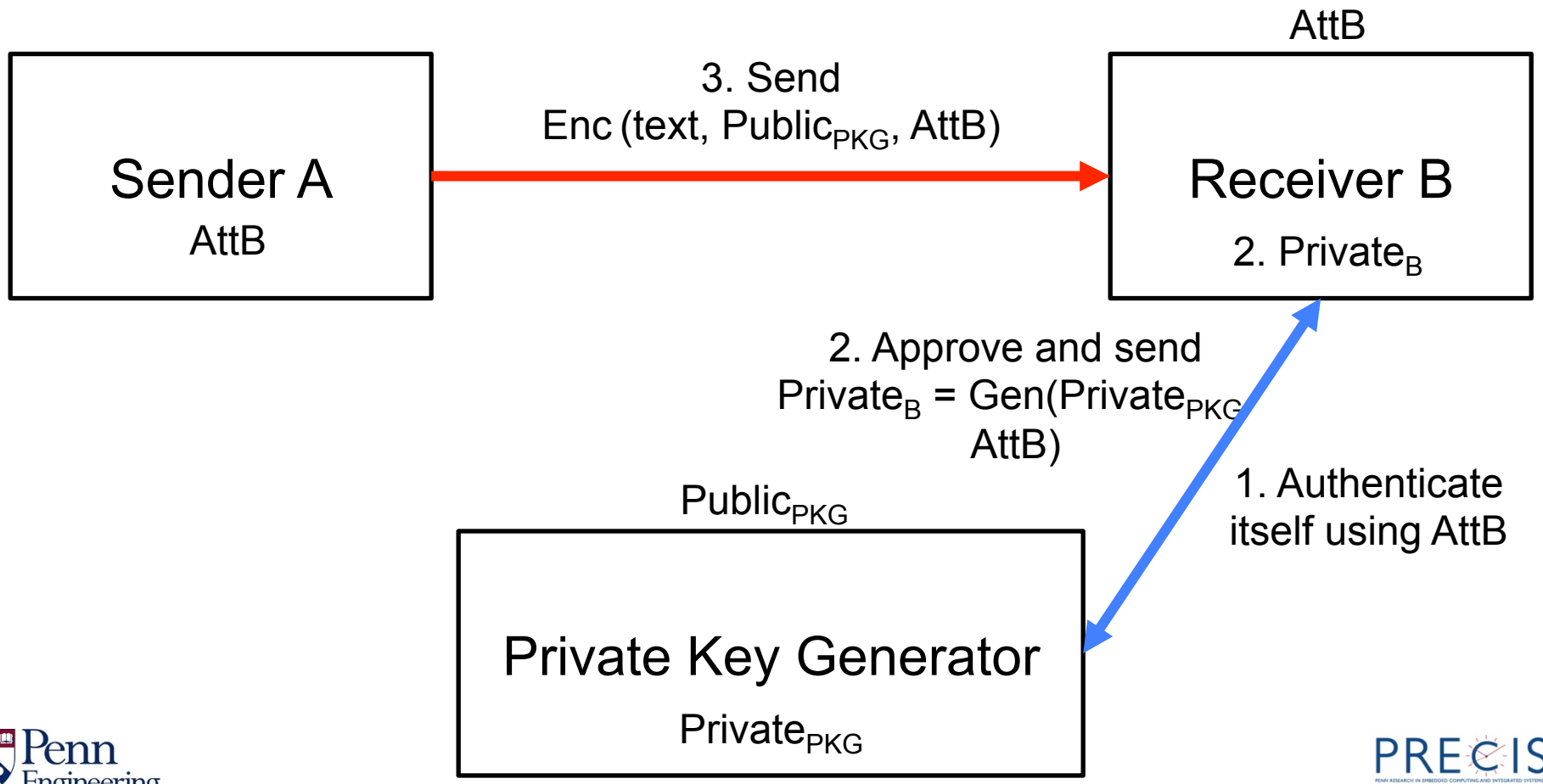
Identity Based Encryption

- Identity of a receiver
  - ID of the receiver



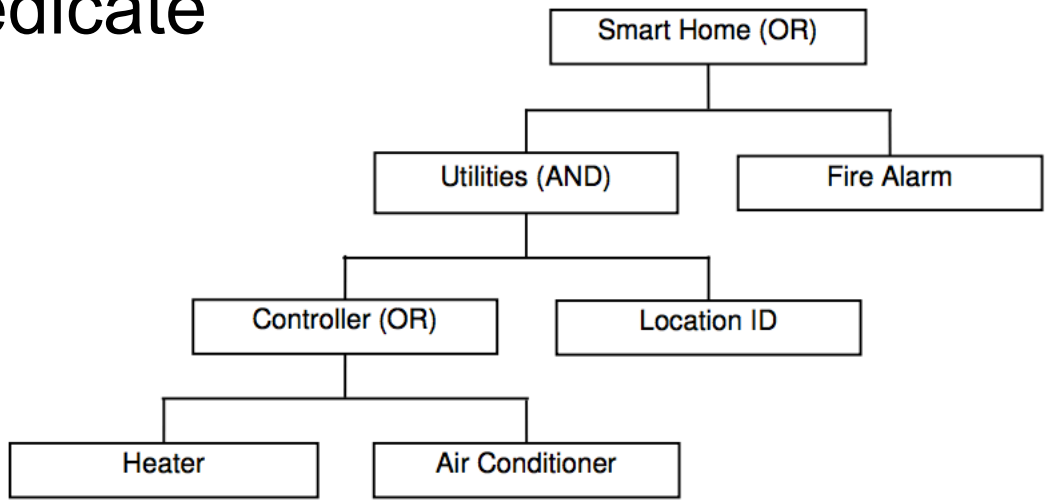
Attribute Based Encryption (ABE)

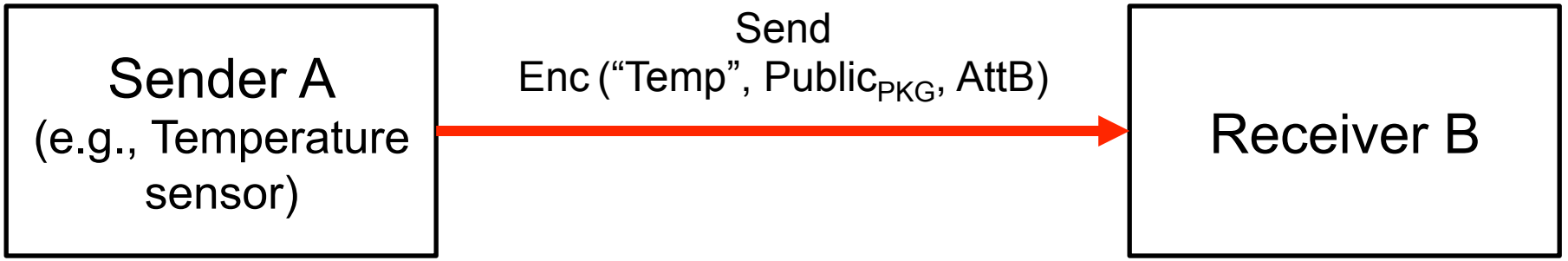
- Identity of a receiver
  - Attributes of the receiver



Attributes

- An attribute of receivers
  - A predicate



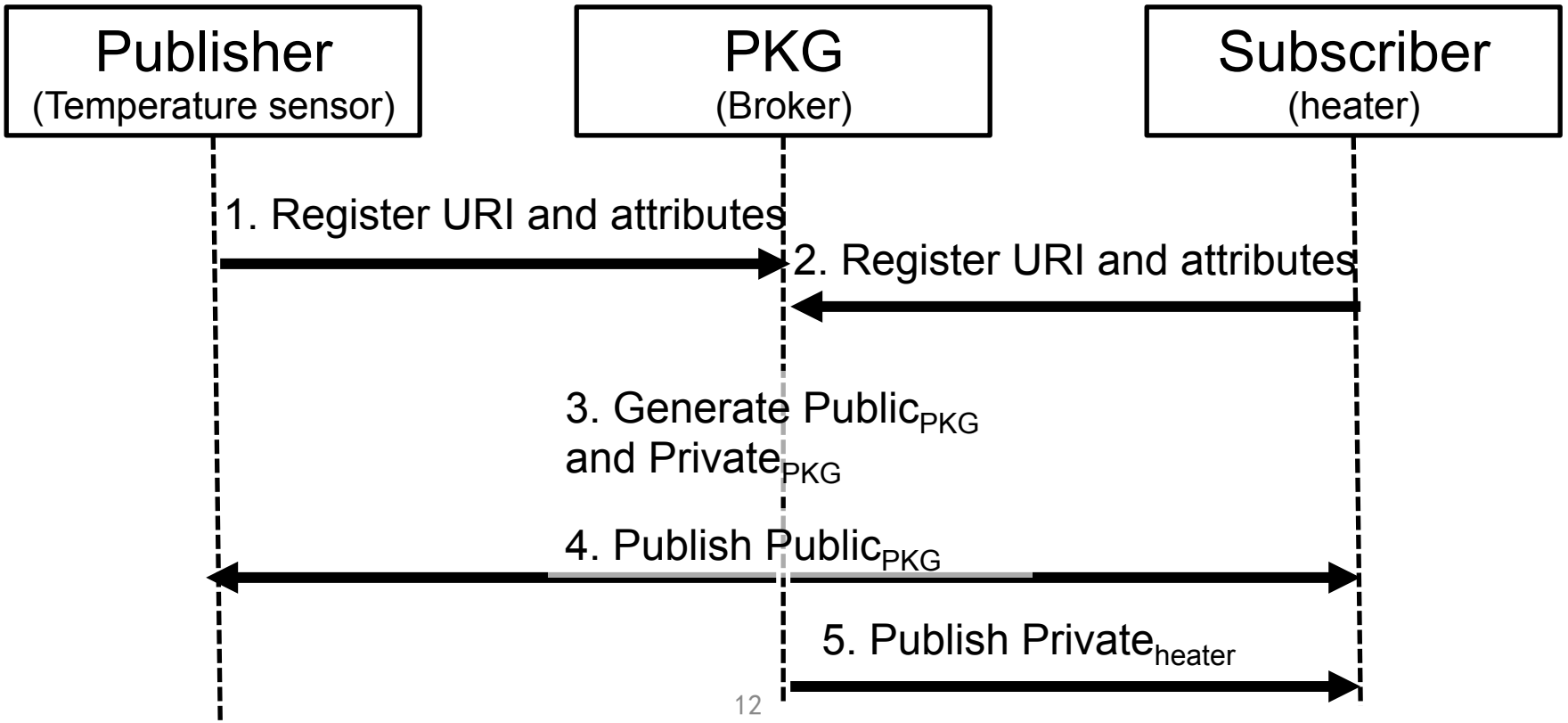


Proposed Secure MQTT (SMQTT)

- SMQTT = MQTT+ABE
  - Update MQTT protocol for ABE
  - Use the ABE scheme based on lightweight Elliptic Curve Cryptography
  - Types of ABE
    - Ciphertext-Policy ABE (CP-ABE)
    - Key-Policy ABE (KP-ABE)

SMQTT Protocol

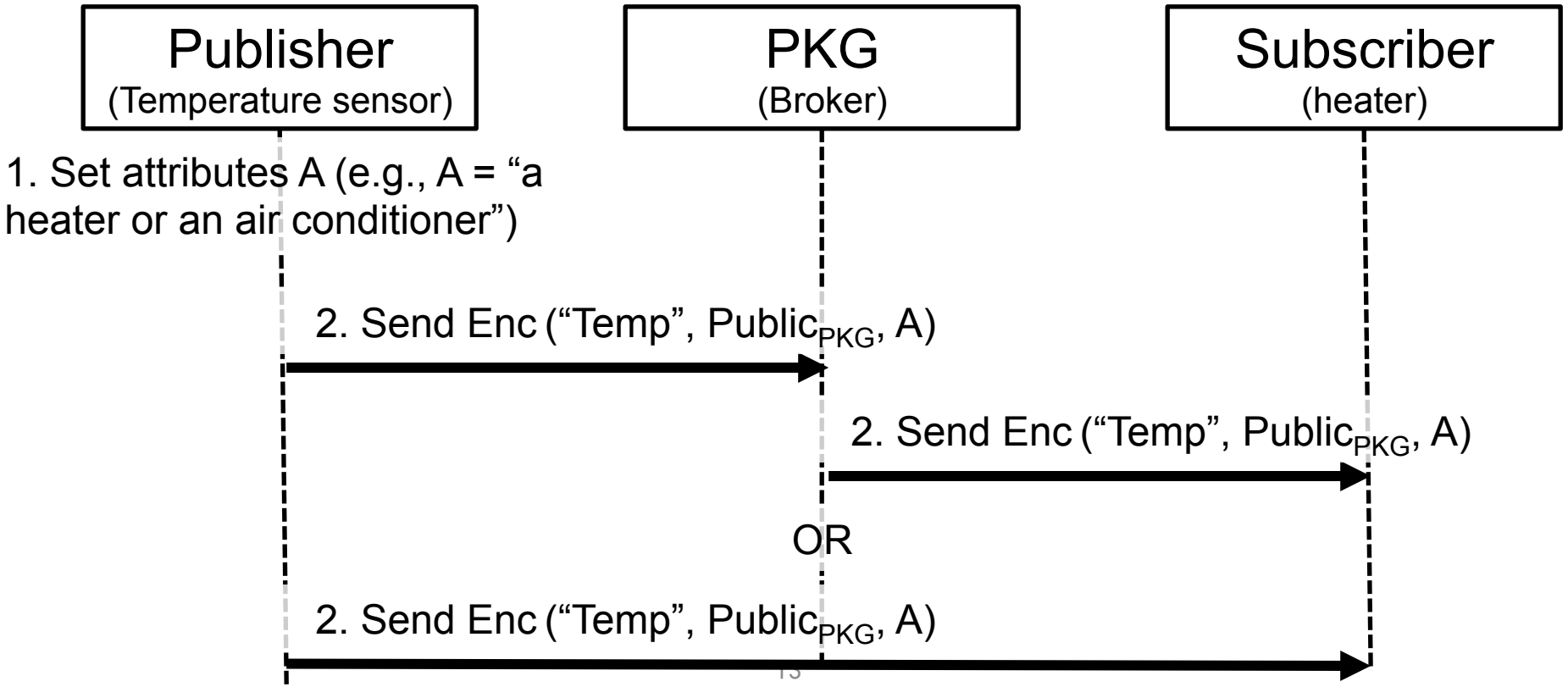
- Setup phase



Note. The universe of all attributes U is known for all entities

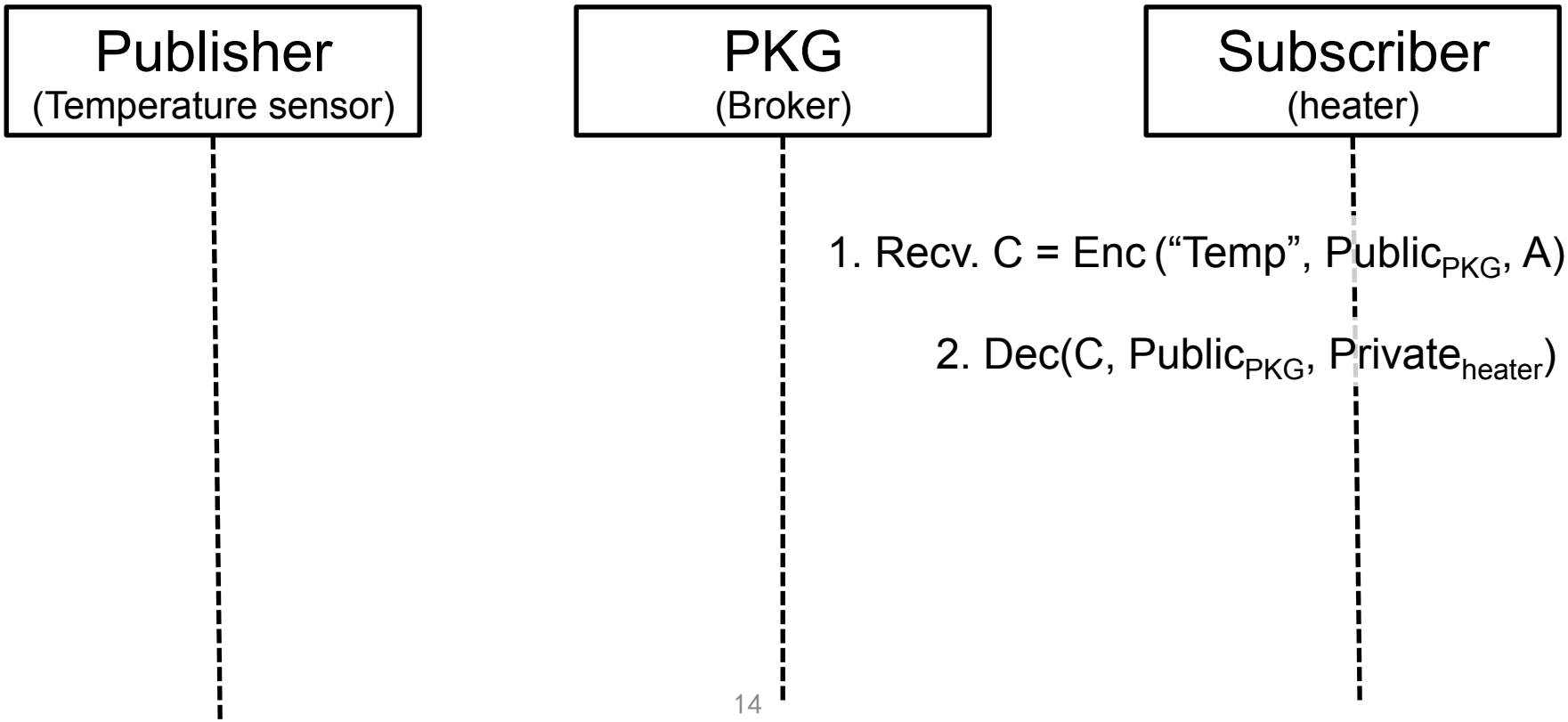
SMQTT Protocol

- Encryption/Publish phase



SMQTT Protocol

- Decryption phase



Performance Analysis

- System details

Hardware	Intel Core DUO CPU@3Ghz
Primary Memory capacity	2 GB
Operating System	Windows 7, 32bit, Linux Mint 13
Java version	1.6
MQTT version	3.1
Broker version	Mosquitto Broker 1.2
Client (Publisher and Subscriber)	Eclipse Paho client 0.9

- Setup phase time of PKG

TABLE VI: Set up Time for KP/CP-ABE

Key Size	KP-ABE (ms)	CP-ABE (ms)
256 bits	187	588
512 bits	4307	19177

Discussion

- Pros/Cons of SMQTT protocol for IoT

- Pros
  - Prior key distribution is not required
  - Broadcast encrypted messages

- Cons
  - How does PKG verify the attribute of a receiver?
    - “PKG verifies attributes and other details given by the device”
    - Any adversary can claim any attributes