# Key Generation From Wireless Channels Lightweight Security for Internet of Things

Junqing Zhang
junqing.zhang@liverpool.ac.uk
Department of Electrical Engineering and Electronics,
University of Liverpool

Internet of Things - Connecting Everything Together

Internet of Things (IoT) integrates ubiquitous connections between things with communication, computing, and sensing ability.

7.6 Billion
World population by 2020

50 Billion
Connected devices by 2020

6.58
Devices per person by 2020

£2.94 Trillion
Potential economic impact per year by 2020

Data Source: Cisco

Data Source: McKinsey
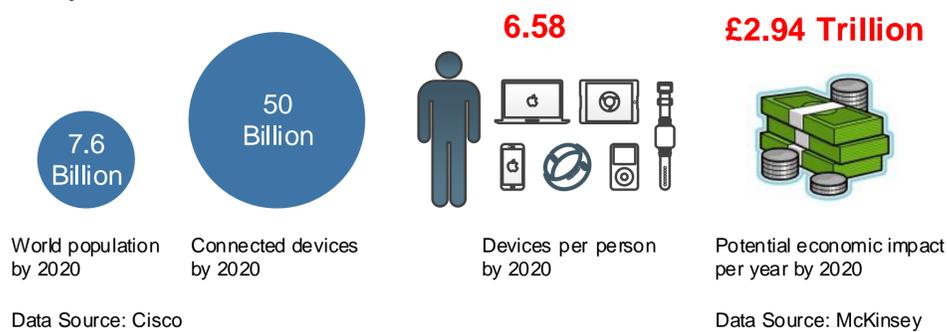
What can you do with Internet of Things?

Smart Home
Your house on your hand

E-commerce
Shopping cannot be easier

Healthcare
Monitor your health all the time

Smart Traffic
Never be late again

and more and more ...
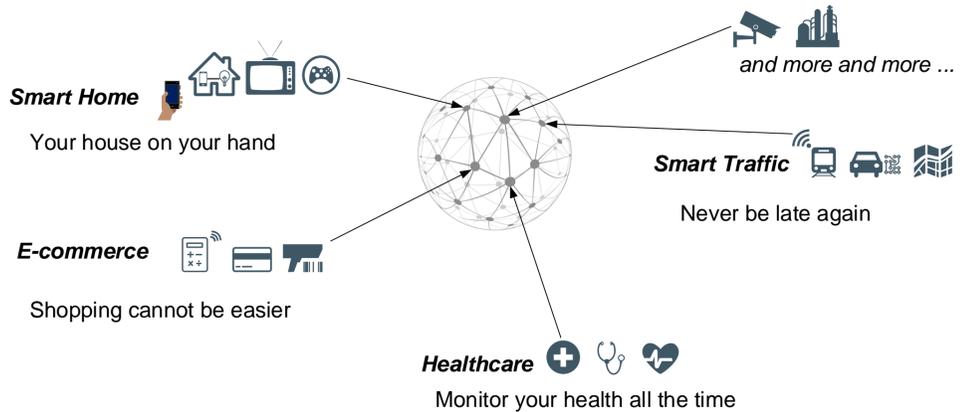
## Security is Challenging for IoT

Conventional encryption system uses public key cryptography to share the key between users.

Public Key
Public Key Infrastructure
Public Key
Private Key a
Private Key b
Public Key Cryptography
Public Key Cryptography
K
K
Encryption
Encryption
Plaintext
Ciphertext
Plaintext
Alice
Eve
Bob
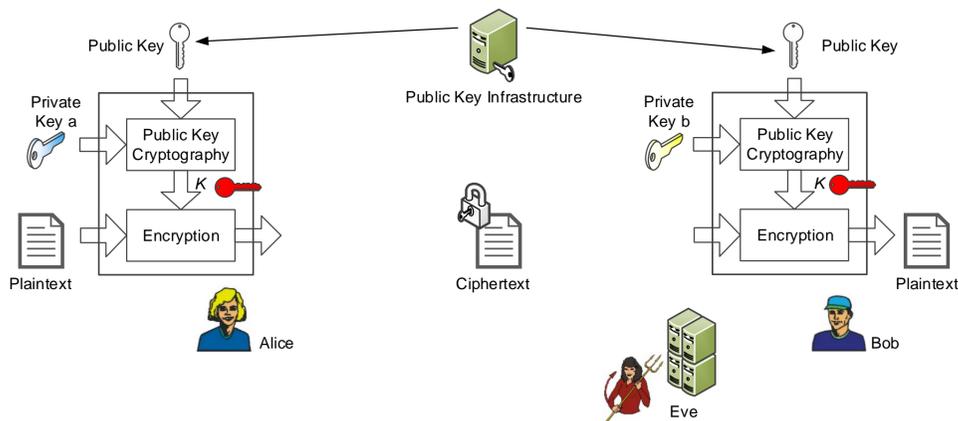
Three issues to apply public key cryptography in IoT:
① Public key infrastructure may not be available.
② Would be cracked by the emerging quantum algorithms.
③ Too heavy for low cost IoT devices.

Use Your Environment as the Key

The wireless environment residing between users is perfect as the key, termed as *physical layer security key generation*.

X
t
X → Key Generation → K
Matching
Y
t
Y → Key Generation → K
Alice

Not Matching

Z
t
Z → Key Generation → ?
Eve

Wireless Channel
Bob
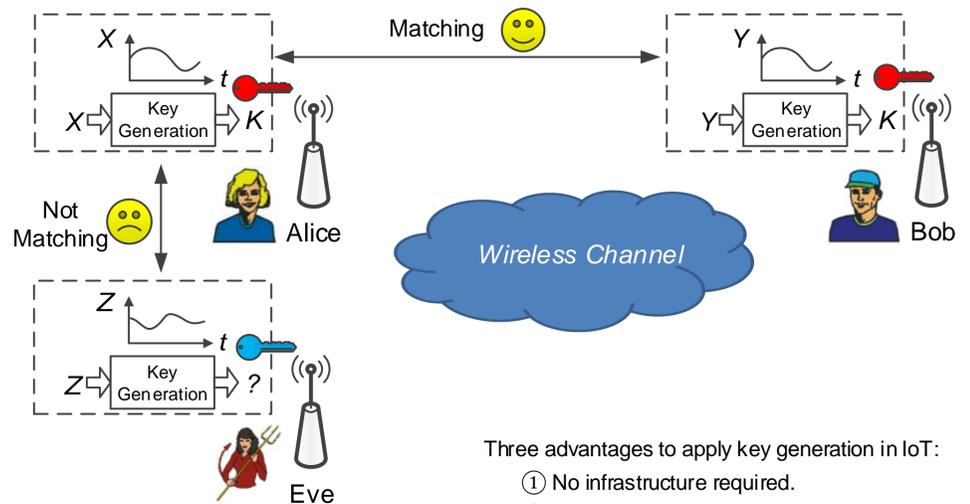
Three advantages to apply key generation in IoT:
① No infrastructure required.
② Perfect secrecy, will never be cracked.
③ Lightweight.

Key Generation Research at Liverpool

Channel Probing
Public pilot
Public pilot
Channel Probing
X^A
X^B
Quantization
Quantization
K_q^A 01001...
K_q^B 01011...
Information Reconciliation
Public discussion, s
Information Reconciliation
K_{ir}^A
K_{ir}^B
Privacy Amplification
Privacy Amplification
K^A
Alice
K^B
Bob
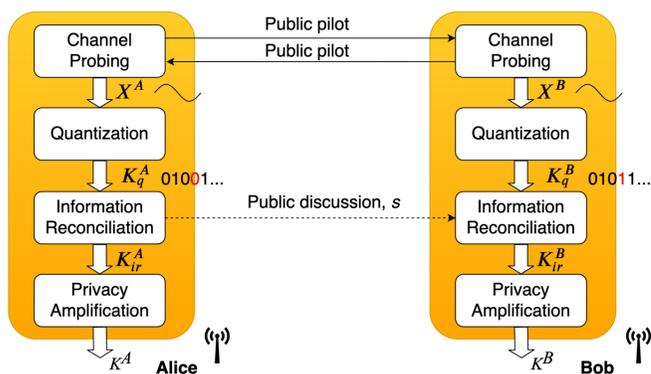
Pairwise Key Generation

Anechoic Chamber, WiFi
Alice
Bob and Eves

Reverberation Chamber, WiFi
Bob and Eves
Stirrer 1
Alice

Urban, LoRa
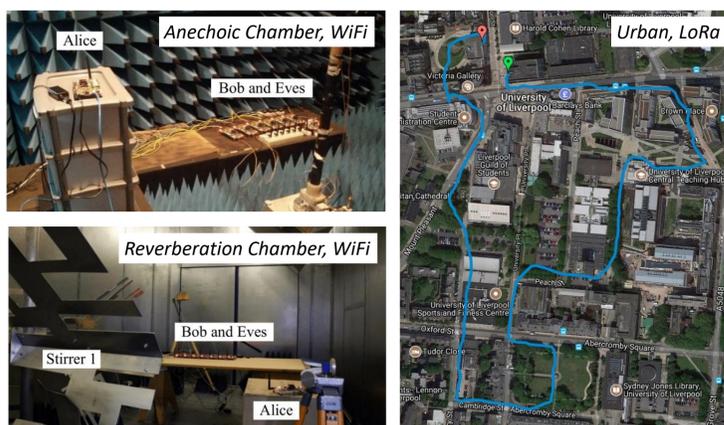
Key Generation Experiments

Received power (dBm)
Alice — Bob — Alice Mean — Bob Mean
Mismatch
Timestamp (s)

Key Generation Results (WiFi)

f_1
f_1 f_2 f_3 f_4
Frequency
Station 1
Station 2
Station 3
Station 4
AP
f_2
f_3
f_4
→ Downlink
⇢ Uplink
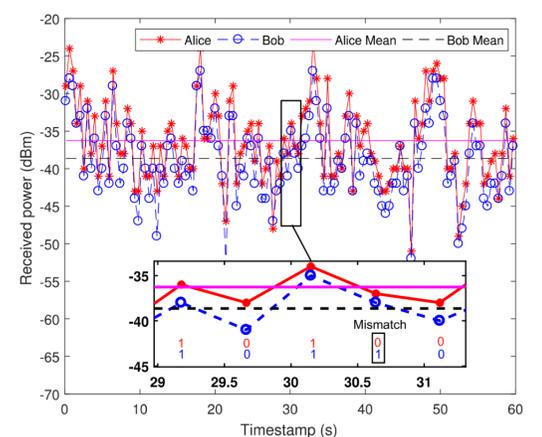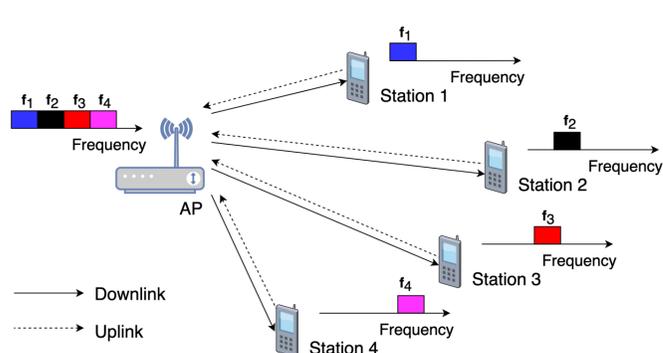
OFDMA-based Multi-User Key Generation

Alice (AP)
Bob (Station)
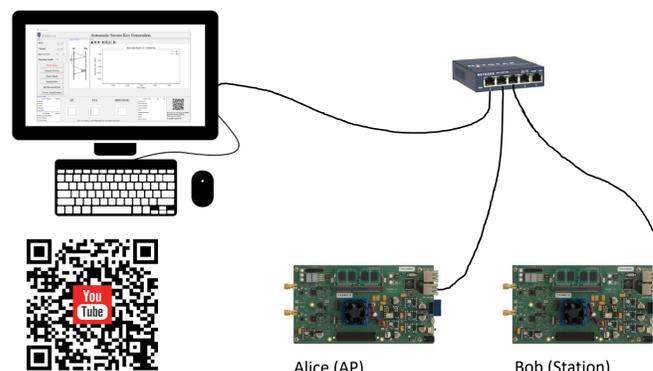
Key Generation Demonstration

Received power (dBm)
Mean-based quantization
Differential-based quantization
Mismatch
Alice — Bob — Alice Mean — Bob Mean
Packet Index

Key Generation Results (LoRa)