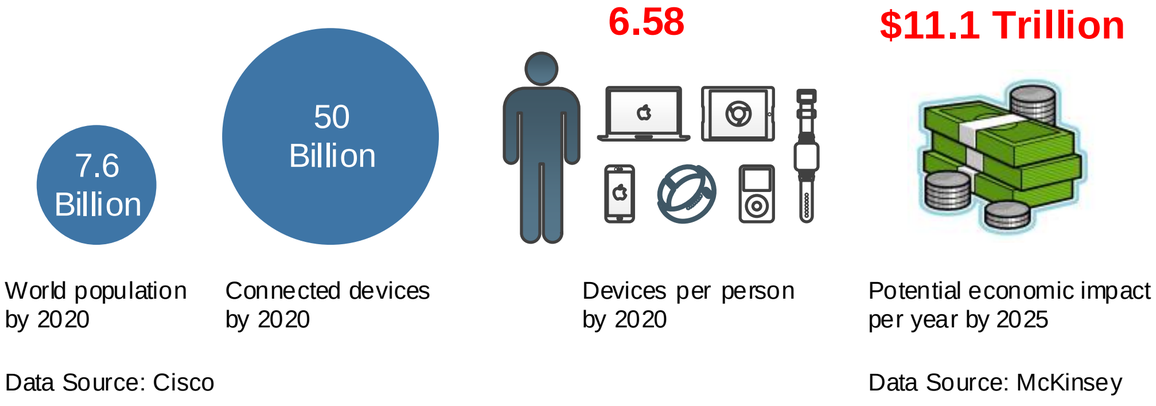
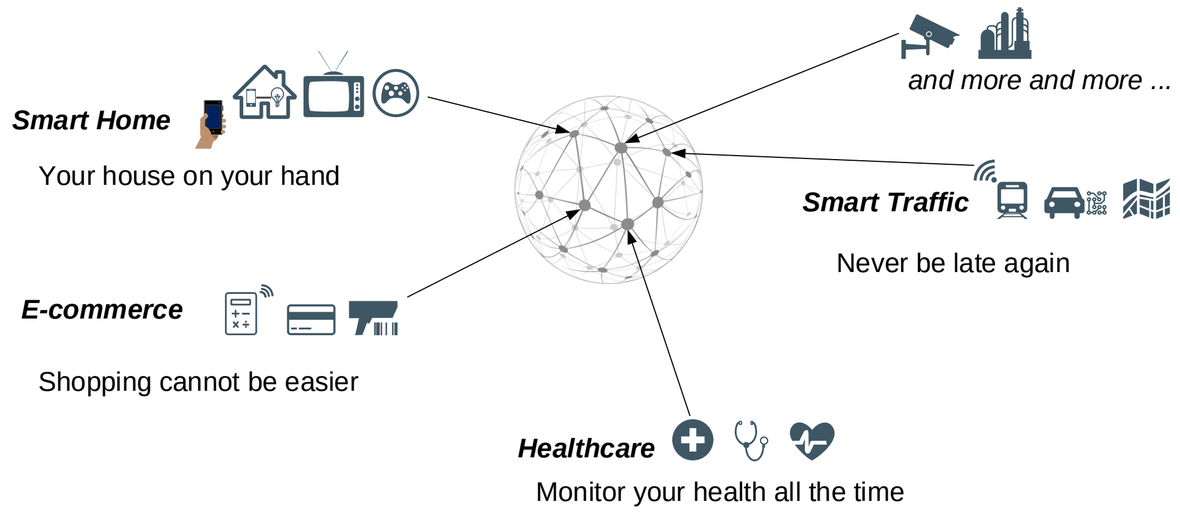
Tackling Cyber Security of Internet of Things by Leveraging Low Cost Physical Layer Security

Junqing Zhang, Roger Woods, and Trung Q. Duong
{jzhang20, r.woods, trung.q.duong}@qub.ac.uk

Internet of Things - Connecting Everthing Together

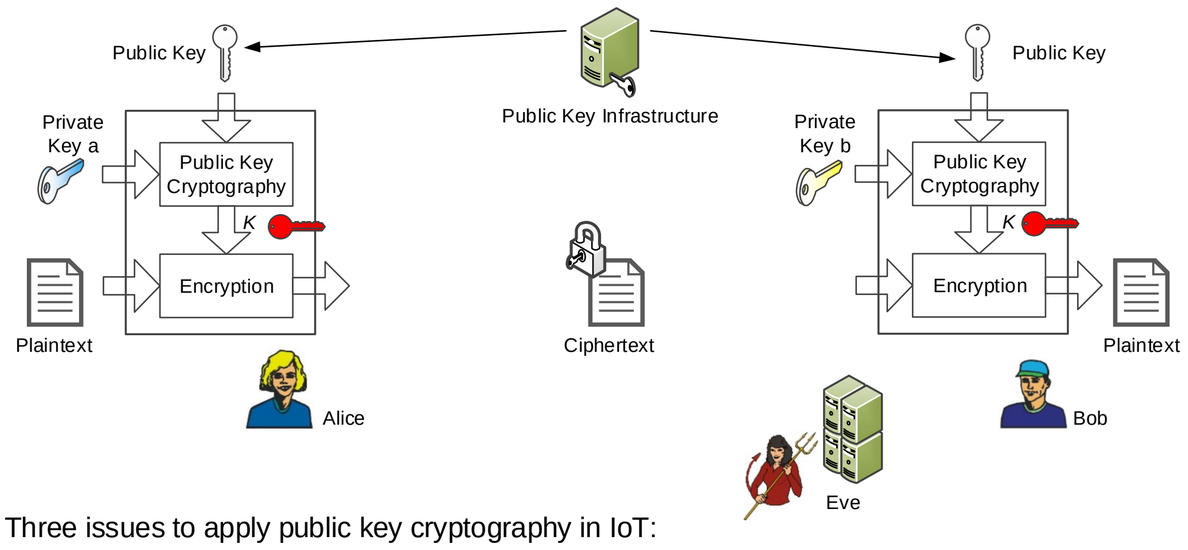
Internet of Things (IoT) integrates ubiquitous connections between things with communication, computing, and sensing ability.





Security is Challenging for IoT

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

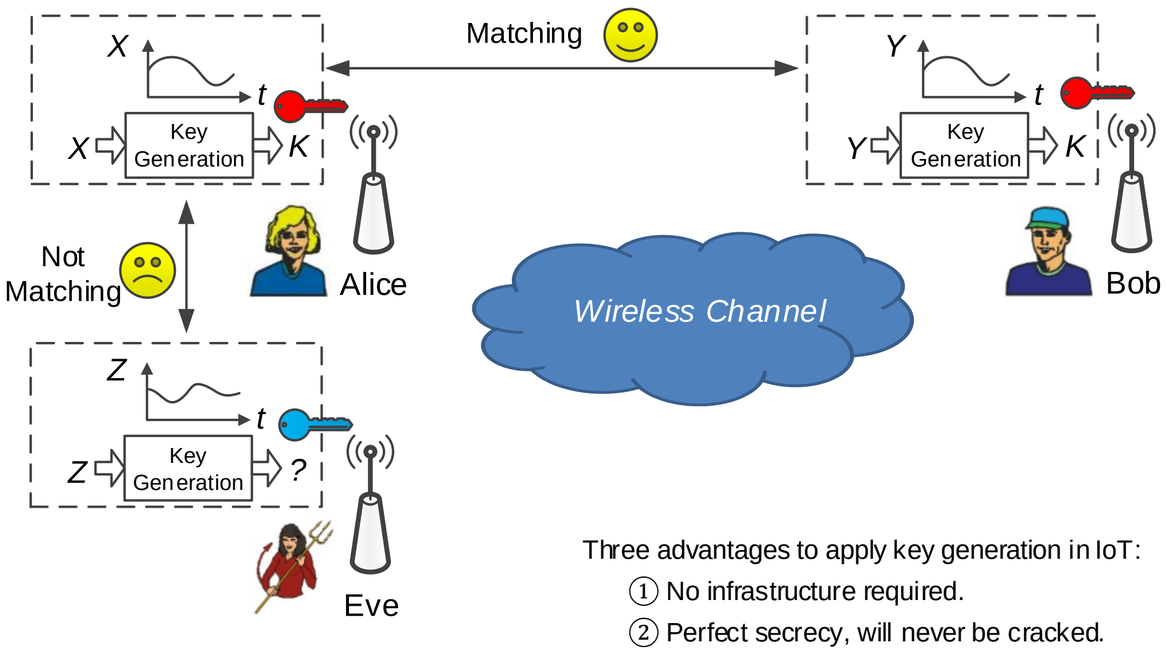


Three issues to apply public key cryptography in IoT:

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*.



Three advantages to apply key generation in IoT:

① No infrastructure required.
② Perfect secrecy, will never be cracked.
③ Lightweight.

Physical Layer Security at Queen's

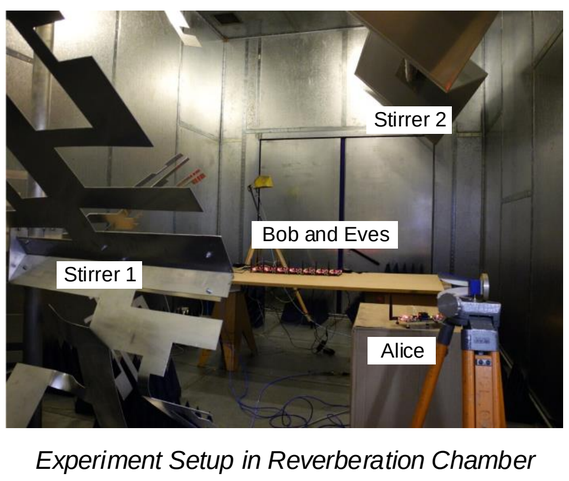
We are dedicated to develop ***lightweight*** and ***"almost free"*** physical layer security key generation for low cost IoT devices. We implemented our ideas using state-of-the-art prototyping facility (WiFi-based WARP technology), and have carried out extensive theoretical and experimental studies.

Research Achievement/Impact

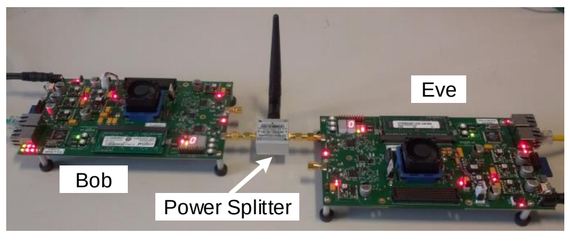
- The first academic research group in the UK working on practical key generation
- Six top-notch journal and five key conference papers
- Four projects under review for potential financial support

Collaborator

Experiment Setup in Anechoic Chamber



Experiment Setup in Reverberation Chamber



Experiment Setup to Study Key Generation Principle

Each square denotes one bit, with black and white representing 1 and 0, respectively

Experiment Results: Key Generated by Users

Acknowledgement

STEM for BRITAIN, 13 March, 2017