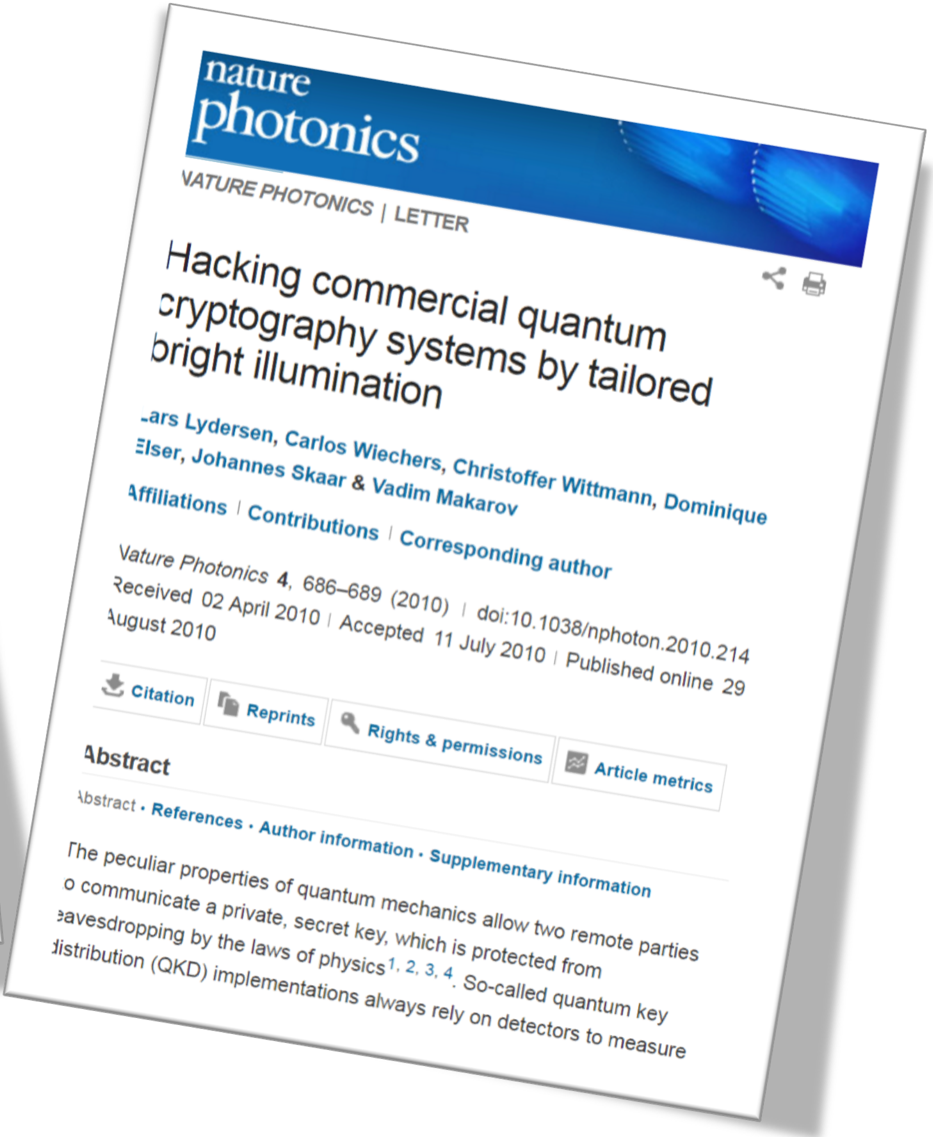
Commissioning Methods for IoT

LARS LYDERSEN | DIRECTOR OF IOT SECURITY

EMBEDDED WORLD FEBRUARY 26–28, 2019

Meet Lars the Quantum Hacker



nature photonics

NATURE PHOTONICS | LETTER

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

Affiliations | Contributions | Corresponding author

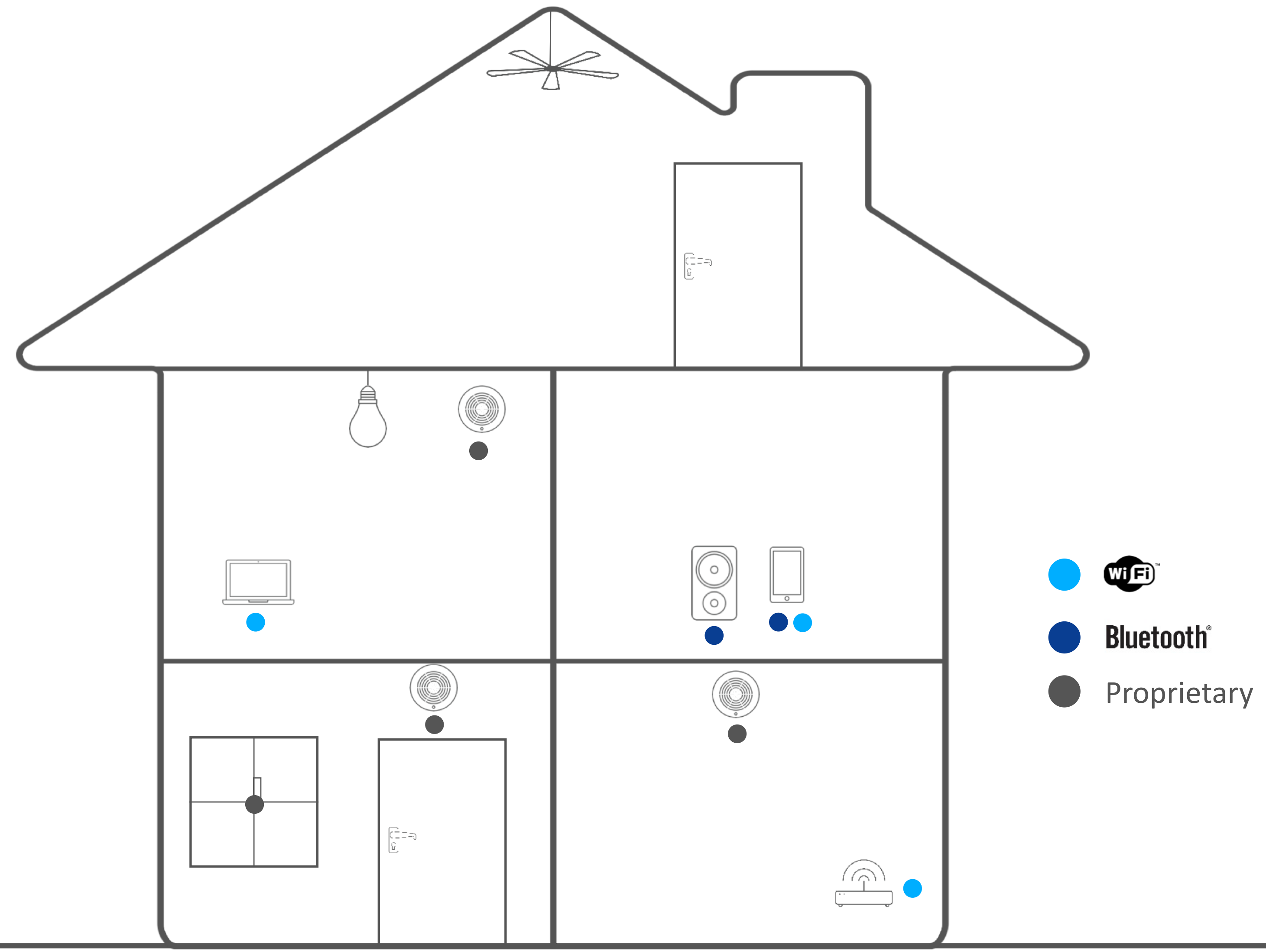
Nature Photonics 4, 686–689 (2010) | doi:10.1038/nphoton.2010.214
Received 02 April 2010 | Accepted 11 July 2010 | Published online 29 August 2010

Abstract

Abstract • References • Author information • Supplementary information

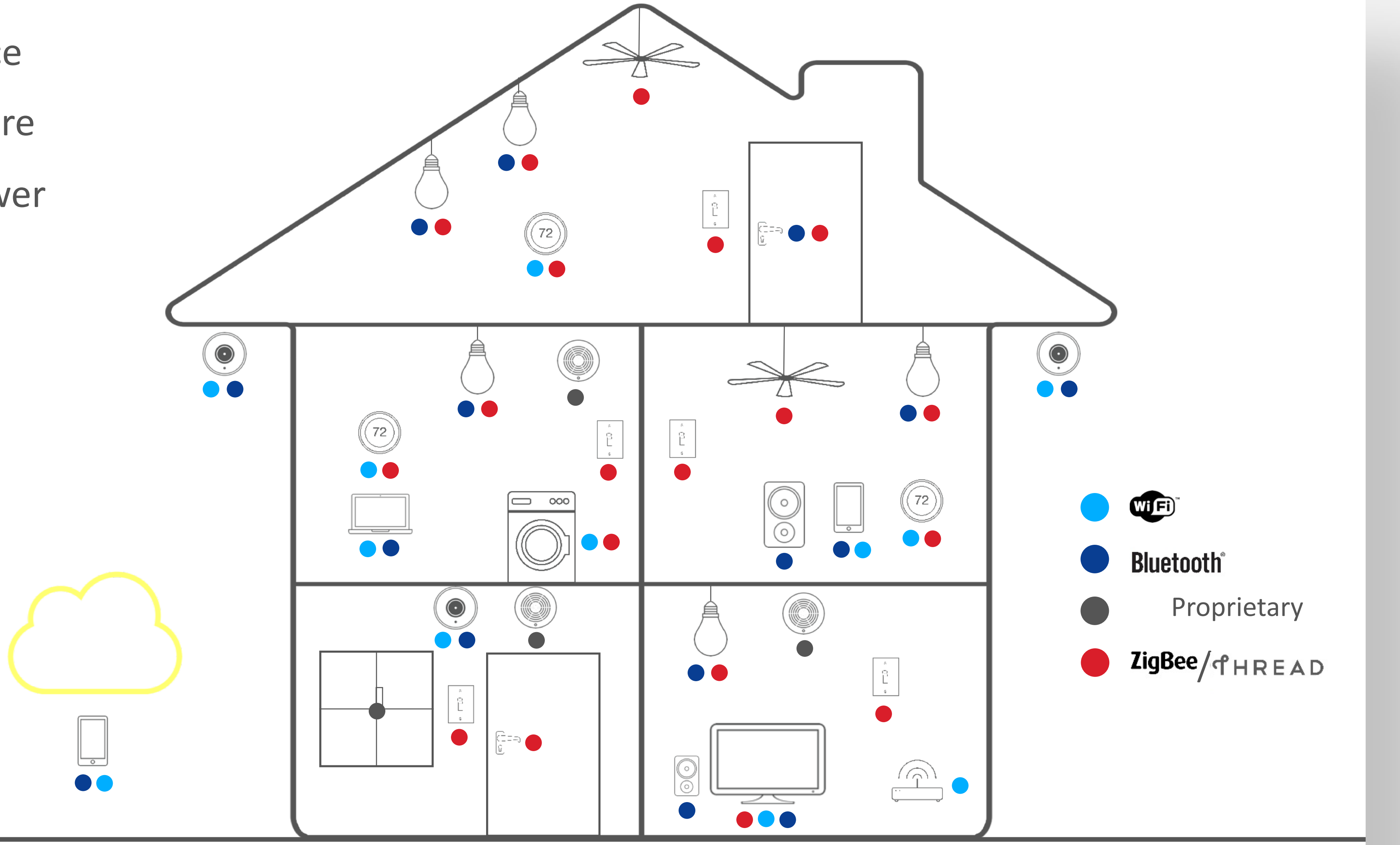
The peculiar properties of quantum mechanics allow two remote parties to communicate a private, secret key, which is protected from eavesdropping by the laws of physics[1, 2, 3, 4]. So-called quantum key distribution (QKD) implementations always rely on detectors to measure

Classical Cyber Security

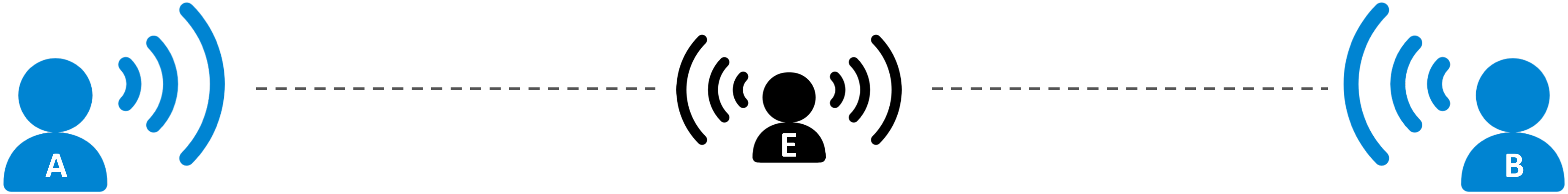


IoT Security

- Increased attack surface
- Accessibility to hardware
- Limited processing power in end nodes



Authentication vs Encryption



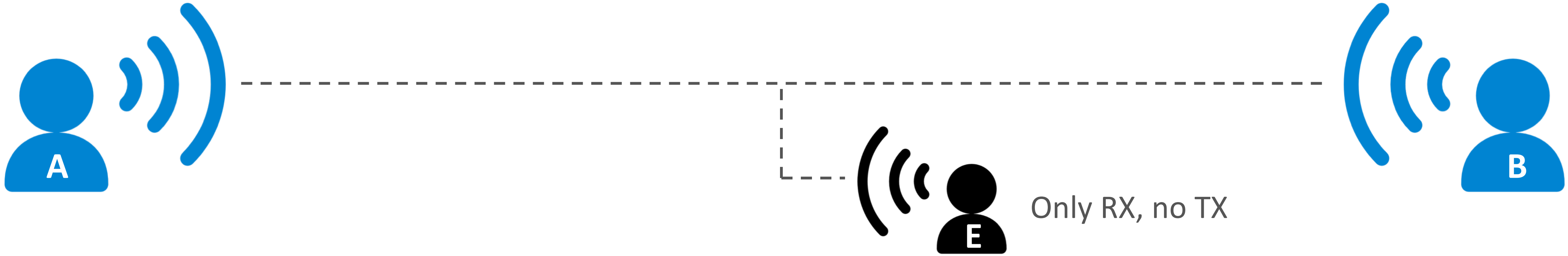
- Lack of authentication = Alice does not know she is talking to Bob
  - Eve can impersonate Alice and/or Bob

- Lack of encryption = anyone can read communication between Alice and Bob
  - In particular, Eve can read this information

- No encryption without authentication
  - If so, Eve can impersonate Bob, and read the information

Authentication vs Encryption

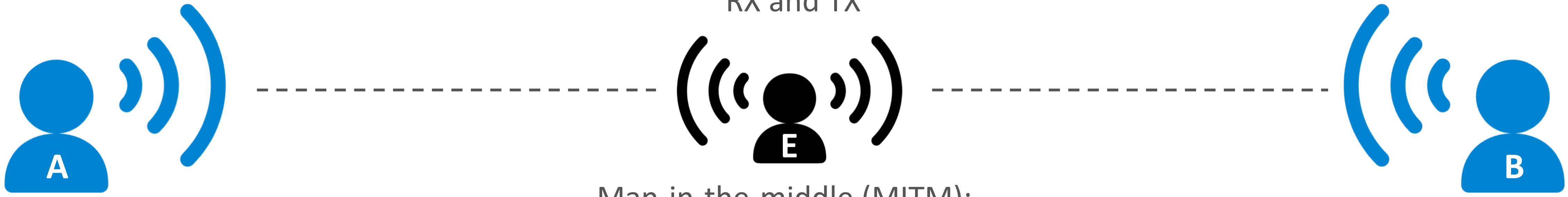
Passive



Only RX, no TX

Active

RX and TX



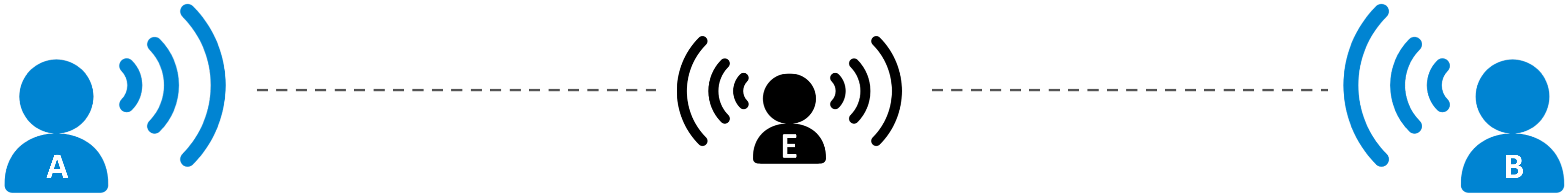
Man-in-the-middle (MITM):
A and B only communicates
via Eavesdropper

IoT Wireless Protocols Becoming More Secure

	Wi Fi		Bluetooth		zigbee	THREAD
	WEP	WPA/WPA2	< v4.2	>= v4.2		
Passive attacker	Insecure	Secure	Window during commissioning	Secure	Window during commissioning	Secure
Active attacker*	Insecure	Secure	Secure	Secure	Insecure if insecure rejoin is enabled	Secure

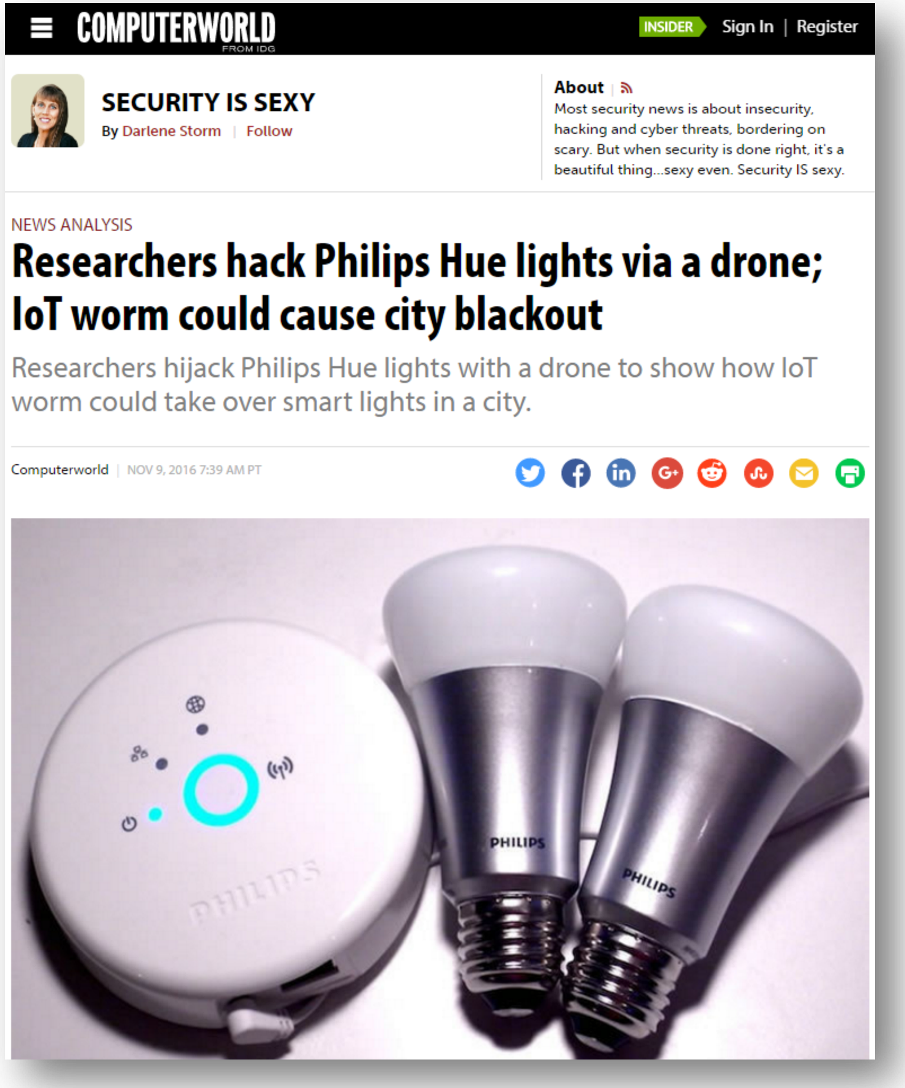
*Disregarding MITM; feasibility of MITM depends on commissioning scheme

The Commissioning Problem



- To secure the link Alice and Bob needs to share a secret key = link/network key
- How to distribute the key?
- Typically combined with accepting a device into the network

A Lightbulb Worm?



COMPUTERWORLD FROM IDG

INSIDER Sign In | Register

SECURITY IS SEXY

By Darlene Storm | Follow

About

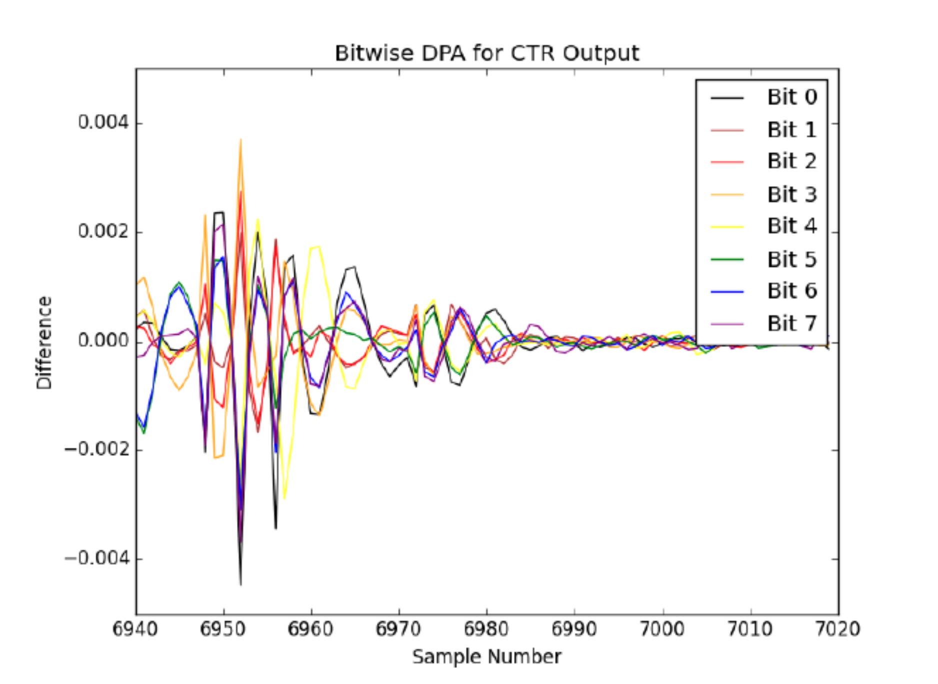
Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

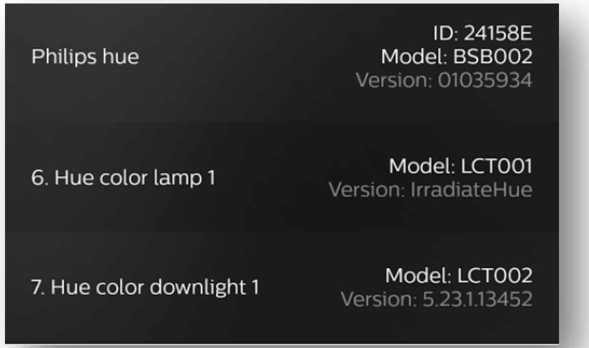
NEWS ANALYSIS

Researchers hack Philips Hue lights via a drone; IoT worm could cause city blackout

Researchers hijack Philips Hue lights with a drone to show how IoT worm could take over smart lights in a city.

Computerworld | NOV 9, 2016 7:39 AM PT





Philips hue	ID: 24158E Model: BSB002 Version: 01035934
6. Hue color lamp 1	Model: LCT001 Version: IrradiateHue
7. Hue color downlight 1	Model: LCT002 Version: 5.23.1.13452

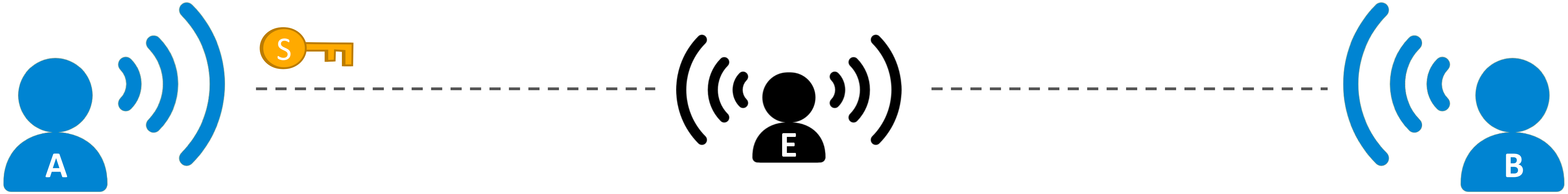
Z-Shave

Security/Privacy is a Balancing Act

- Security/privacy
- Easy of use
- Functionality

General Commissioning Schemes

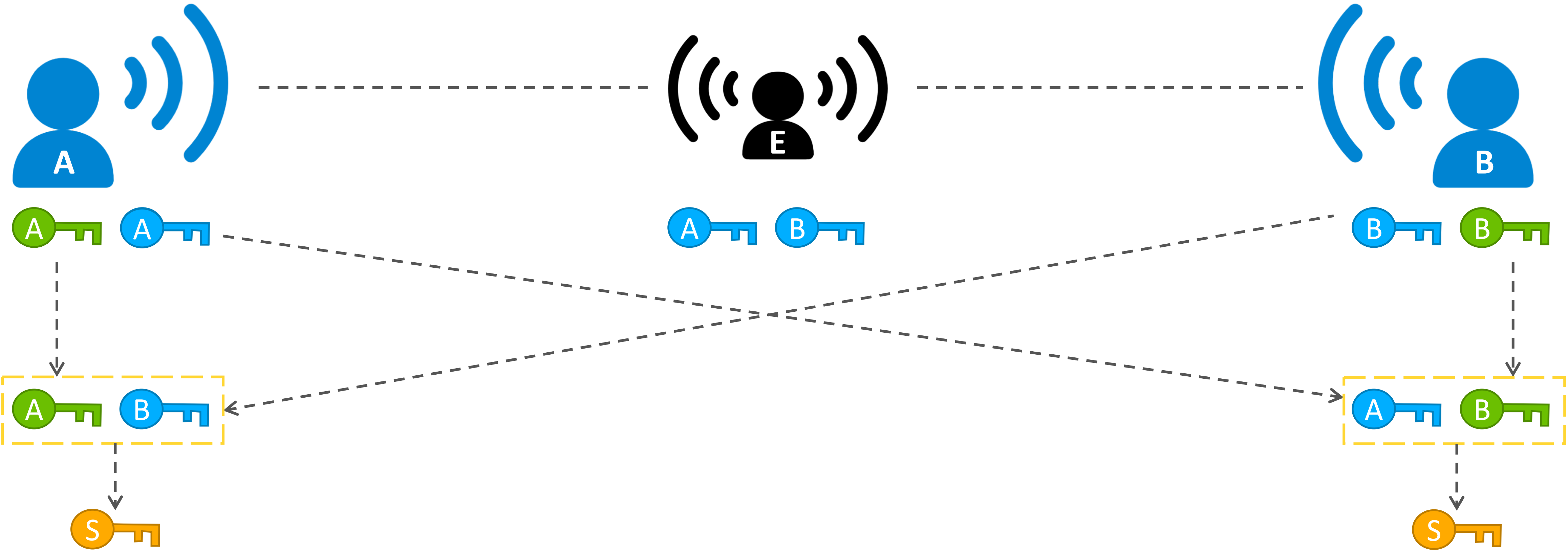
Permissive - Security



- Send the key over the link
  - In clear
  - Encrypted / authenticated with well-known key
  - Via public key cryptography

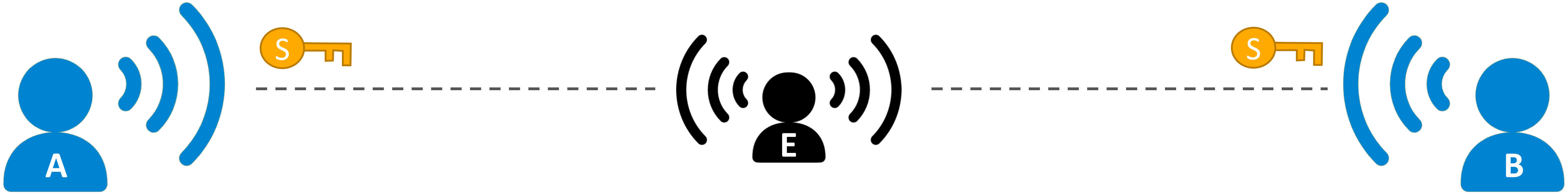
- Security can be improved by
  - Public key cryptography
  - Temporal filtering/windows
  - Spatial filtering/windows

Public Key Based Key Exchange



- Resistant against passive eavesdropping

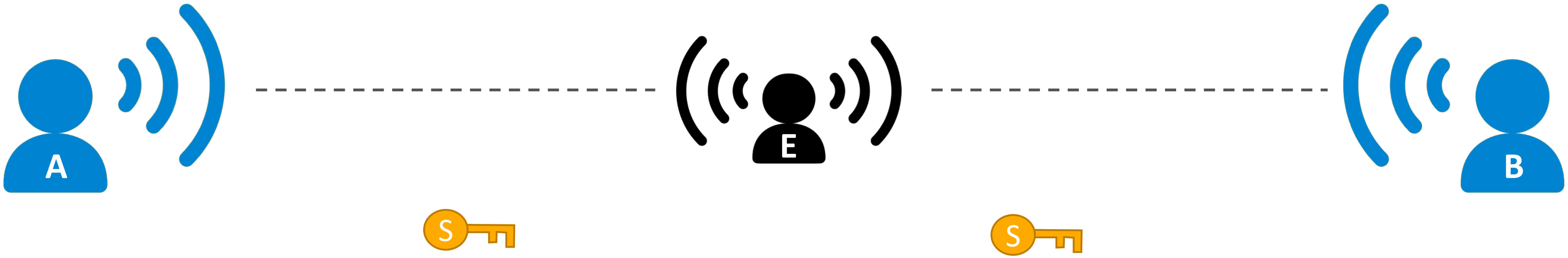
Permissive - Summary



- ✓Easy to use
- ✓Minimal UI requirements
- ✓Minimal operational requirements
- ✓Works fine offline

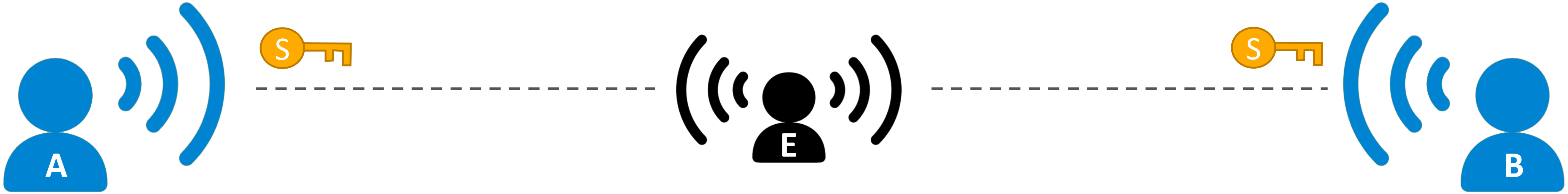
- ✗Level of security

Shared Key - Security



- Key is input into each node
  - User typically inputs the code into one of the nodes
  - Key printed on node?
- Security can be improved by
  - Make long / secure keys efficient – J-Pake, QR-codes etc.
  - Temporal filtering/windows
  - Spatial filtering/windows

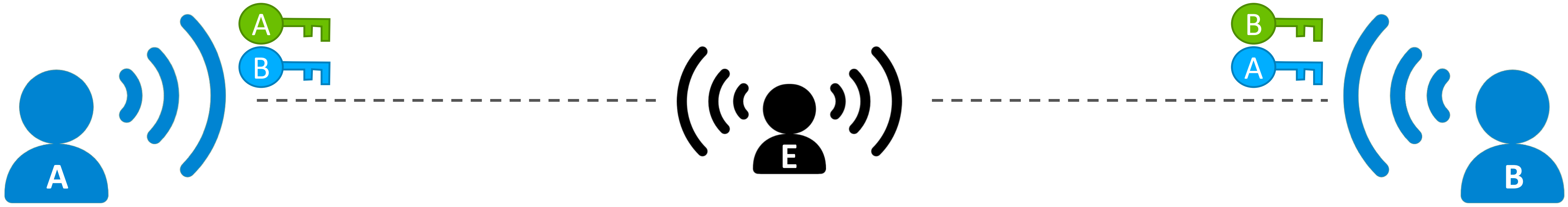
Shared key - Summary



- ✓Can provide good security
- ✓Works offline

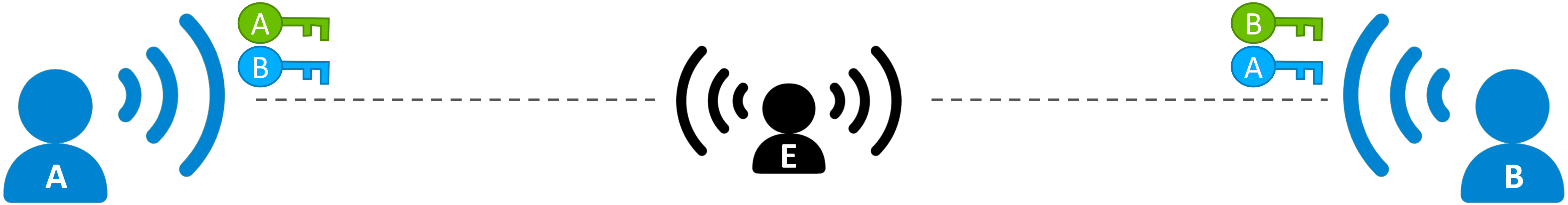
- ✗Requires user interaction
- ✗Can motivate insufficient keys causing insufficient security
- ✗Operational complexity

Certificate-based - Security



- Parties pre-share public keys
  - Public key + meta data = certificate
  - Flexibility to grant rights and sign other certificates

Certificate-based - Summary



- ✓ Very good and flexible security
- ✓ No user interaction / UI

- ✗ Significant operational complexity
- ✗ May not work offline / semi-connectivity
- ✗ Requires more resources from devices

Summary

	Permissive	Shared Key	Certificate-based
Security	✗	✓	✓
Simplicity	✓	✗	✓
UI requirements	✓	✓	✓
Operational requirements	✓	✓	✗
Offline	✓	✓	✓

Standard Schemes in Protocols

WiFi Commissioning Methods

- WPA/WPA2 = shared key method
  - Important to use long keys
  - Note: shared for all devices
- WPS = permissive / shared key method
  - Must support button press
  - Must support 8-digit PIN entry code
  - Support out-of-band
  - WPS is not recommended because PIN entry code has been broken
- WPA Enterprise = shared key / certificate-based method
  - Individual keys per device
  - Requires extra UI, and is not supported on many IoT-devices

Bluetooth (>v4.2) Commissioning Methods

- Public key based key exchange since v4.2
  - Resistant to passive eavesdropping
- Standard methods
  - “Just-works”
    - Permissive method
  - Numeric comparison
    - Shared key
    - Compare two 6-digit numbers on the two devices
  - Passkey entry
    - Shared key
    - Enter 6-digit number displayed on the other device
  - Out-of-band
    - Discussed later

Bluetooth commissioning methods

		Initiator UI				
		Display Only	Display, Yes/No input	Keyboard Only	No Input, No Output	Keyboard, Display
Responder UI	Display Only	Just Works	Just Works	Passkey Entry	Just Works	Passkey Entry
	Display, Yes/No input	Just Works	Numeric Comparison	Passkey Entry	Just Works	Numeric Comparison
	Keyboard Only	Passkey Entry	Passkey Entry	Passkey Entry	Just Works	Passkey Entry
	No Input, No Output	Just Works	Just Works	Just Works	Just Works	Just Works
	Keyboard, Display	Passkey Entry	Numeric Comparison	Passkey Entry	Just Works	Numeric Comparison

Zigbee Commissioning Methods

- Zigbee Home Automation (HA)
  - Permissive
  - Sends key using fixed key
- Zigbee v3.0 extra options
  - Adds option for unique shared key (install codes)
  - Option to replace fixed key with unique key per device
- Zigbee Light Link (ZLL)
  - Permissive
  - Added security using RSSI / proximity window
- Zigbee Smart Energy
  - Public key based, shared key method
  - Unique shared secrets / install codes per device
- All support out-of-band

Thread commissioning methods

- IP-enabled Mesh protocol
  - Allows end-to-end with IP connected devices
- Secret key method
  - Short install codes, unique per device
  - Using J-PAKE to increase security for short codes
  - DTLS is used to secure link during commissioning
- Supports out-of-band
- Further profiles are still in specification

THREAD

Z-Wave commissioning methods

- Mesh protocol by the Z-Wave Alliance
- Designed for home and building automation
- Backwards compatible
- Commissioning method has evolved with protocol versions:
  - < S0:
    - No security during commissioning (no encryption in protocol)
  - S0:
    - Permissive with well-known key (0)
  - S2:
    - Public key based key exchange using ECC Curve25519
    - User may validate public key during commissioning (comparing key at box and controller)
    - SmartStart allows system manufacturer to pre-commission by pushing keys to controller

Out-of-band schemes

- Out-of-band = commissioning method not from standard
- Use one standard to commission another
  - Example: Use Bluetooth “Justworks” to commission ZigBee node
- Near-field communication (NFC)
  - Physical link requires physical proximity
  - Makes MITM more complicated
  - Possible to use public-key based key exchange over NFC

Final remarks

- Commissioning requires challenging tradeoff
  - Security
  - Usability / UI requirements
  - Operational complexity
- Commissioning method categories
  - Permissive
  - Shared key
  - Certificate-based
- Major wireless standards support different methods
  - In general provides interoperability
  - All standards support out-of-band
  - Don’t roll your own unless you have to

Thank You!

LARS LYDERSEN | EMBEDDED WORLD| 27 FEBRUARY 2019