Horst Görtz Institute for IT-Security

RUB

Preventing Scaling of Successful Attacks: A Cross-Layer Security Architecture for Resource-Constrained Platforms

BalkanCryptSec 2014

Istanbul, October 16, 2014

Christian T. Zenger, Abhijit Ambekar, Fredrik Winzer, Thomas Pöppelmann, Hans D. Schotten, Christof Paar

Supported by:

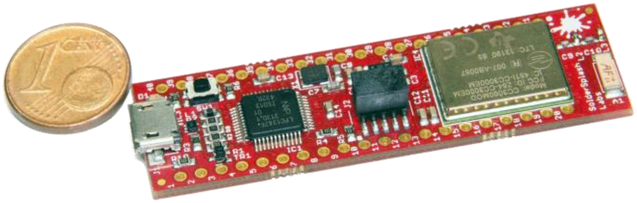
Federal Ministry of Education and Research

Outline

- Motivation
- Physical Layer Security (PHYSEC)
- Experimental Results
- PHYSEC meets asymmetric Cryptography

Motivation

- How to establish secret keys into tiny IoT-devices?



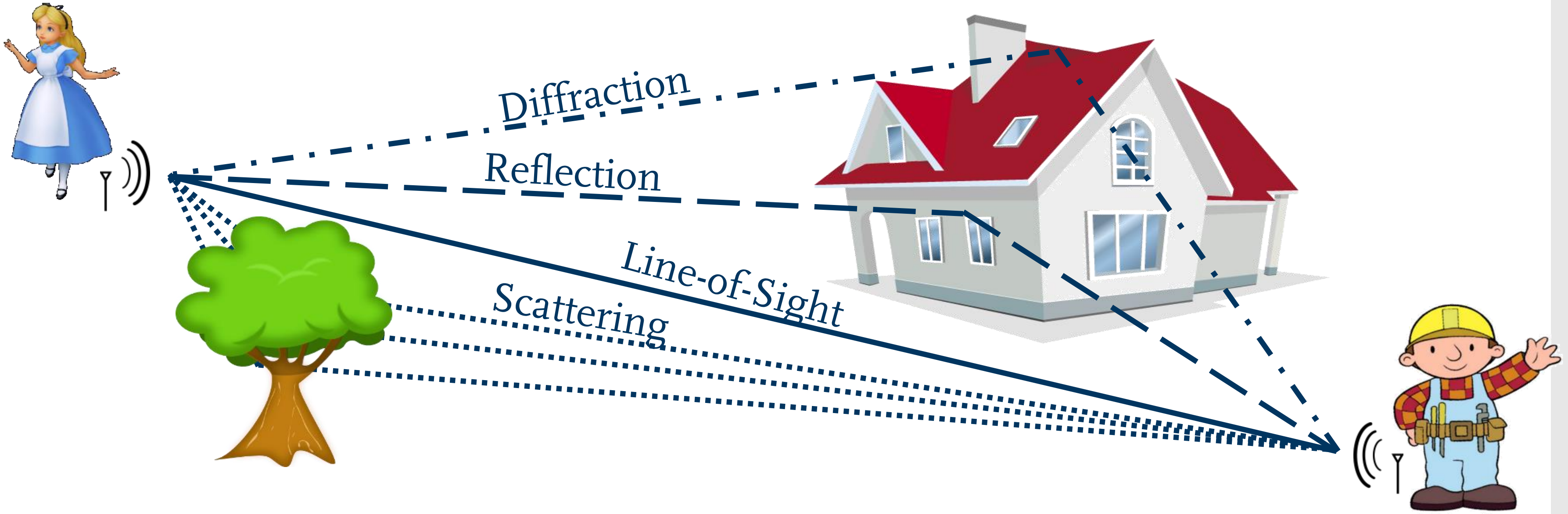
- Without user interfaces
- Under resource- and energy constraints
(due to hardware limitations and battery lifetime)

Motivation:
Key Distribution and Management

- **Symmetric cryptography**
  - Pre-shared keys entails inflexible key distribution and management

- **Asymmetric cryptography**
  - Dynamic key establishment is very energy consuming

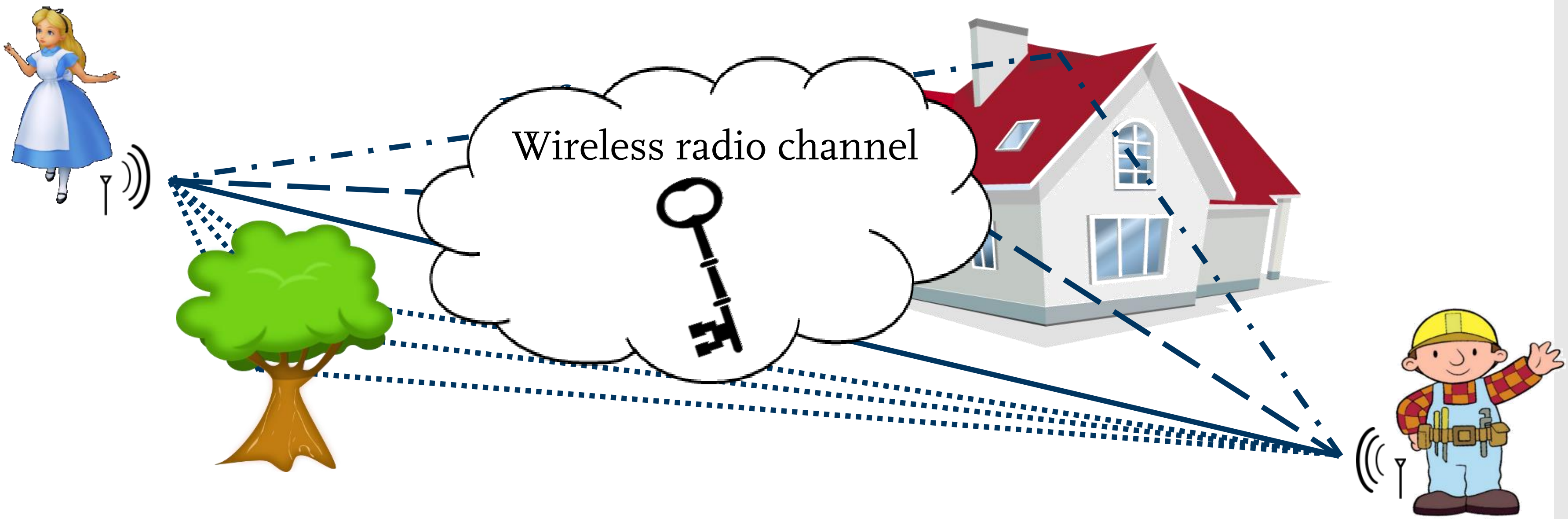
Wireless Channel as Key Variable



- Alice and Bob measure a superposition of different multipath propagations.
- Wireless channel is **easy to estimate**, e.g. by computing the channel impulse response (CIR).
- But the wireless channel is **hard to predict**, especially in presence of movement.

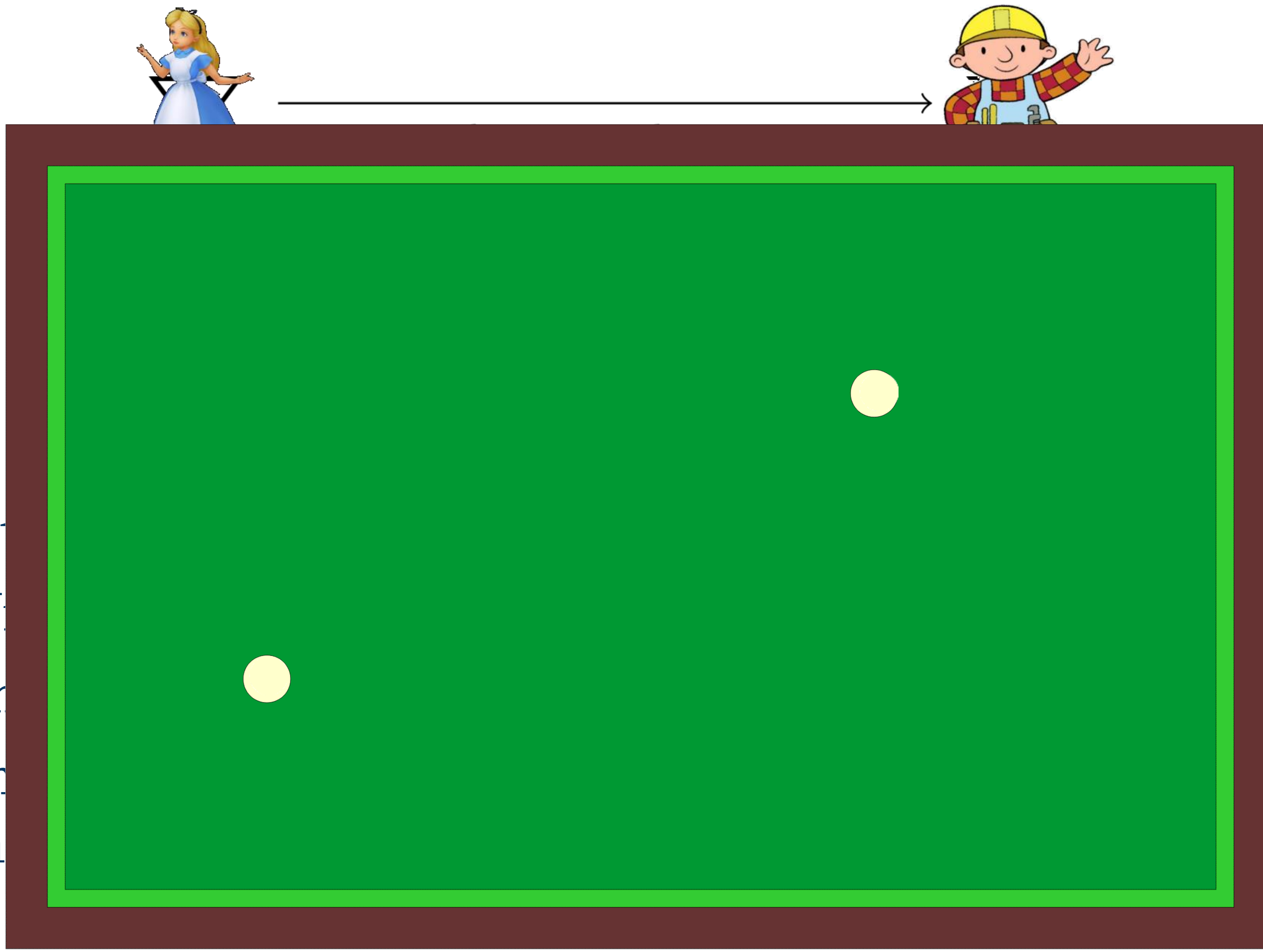
Wireless Channel as Key Variable

RUB



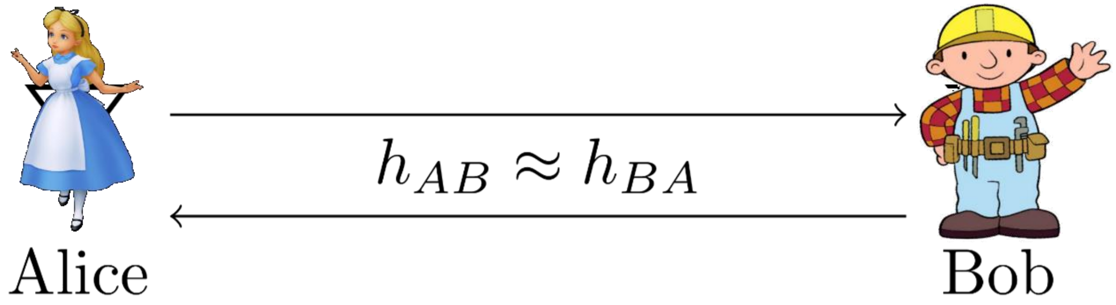
- Alice and Bob measure a superposition of different multipath propagations.
- Wireless channel is **easy to estimate**, e.g. by computing the channel impulse response (CIR).
- But the wireless channel is **hard to predict**, especially in presence of movement.

Channel Reciprocity



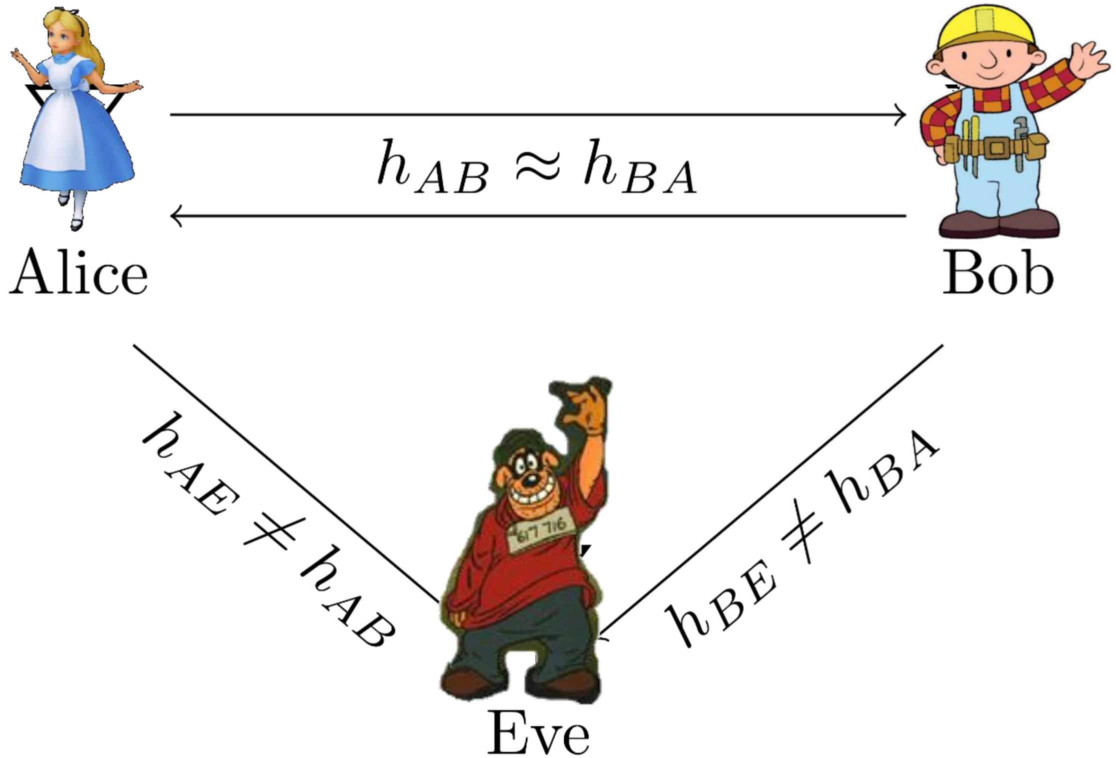
- M
- W
- Ch … me.
- Th
  ch

Channel Reciprocity



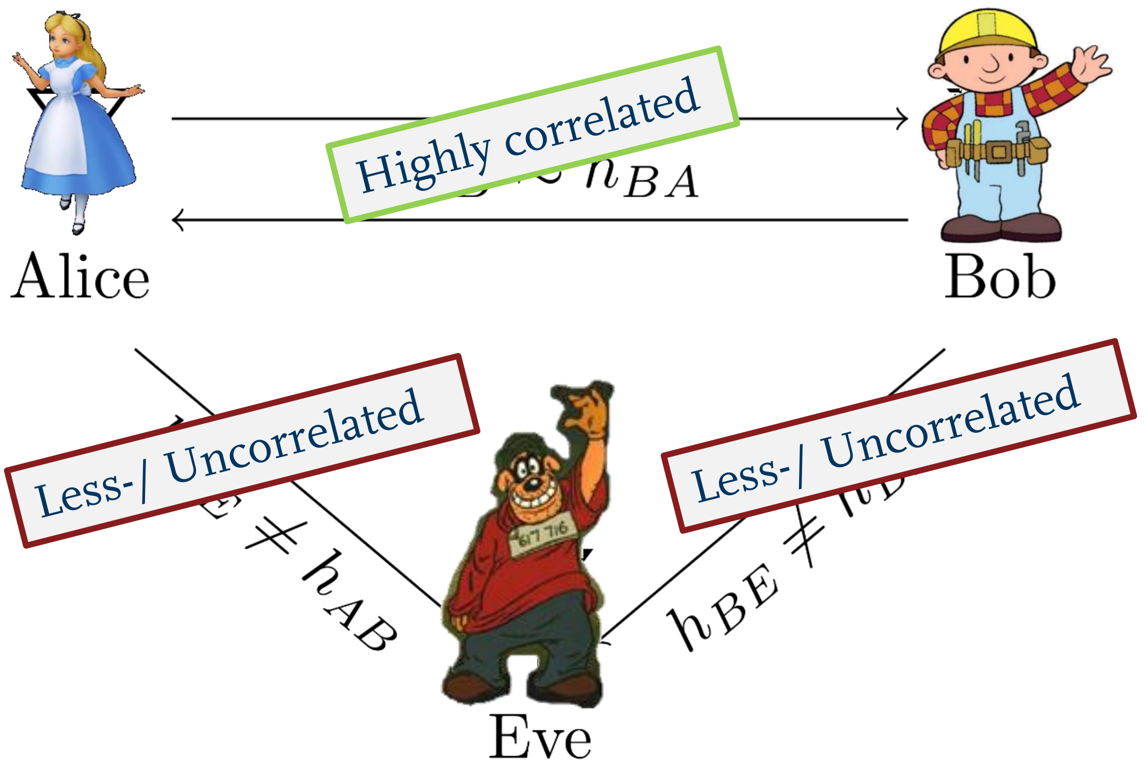
- Multipath propagation is **reciprocal**.
- Wireless **channel varies over time** due to movement.
- Channel could be seen as static within the coherence time.
- The coherence time depends on the velocity within the channel, e.g., for a velocity of 2 m/s it is 63.5 ms.

Channel Diversity



- Multipath propagation varies in space.
- Receiver at different positions estimate different channels.
- The channel decorrelates over the coherence distance $\lambda/2$.
- e.g., for a carrier frequency of 2.4 GHz $\lambda/2 = 6.25$ cm.

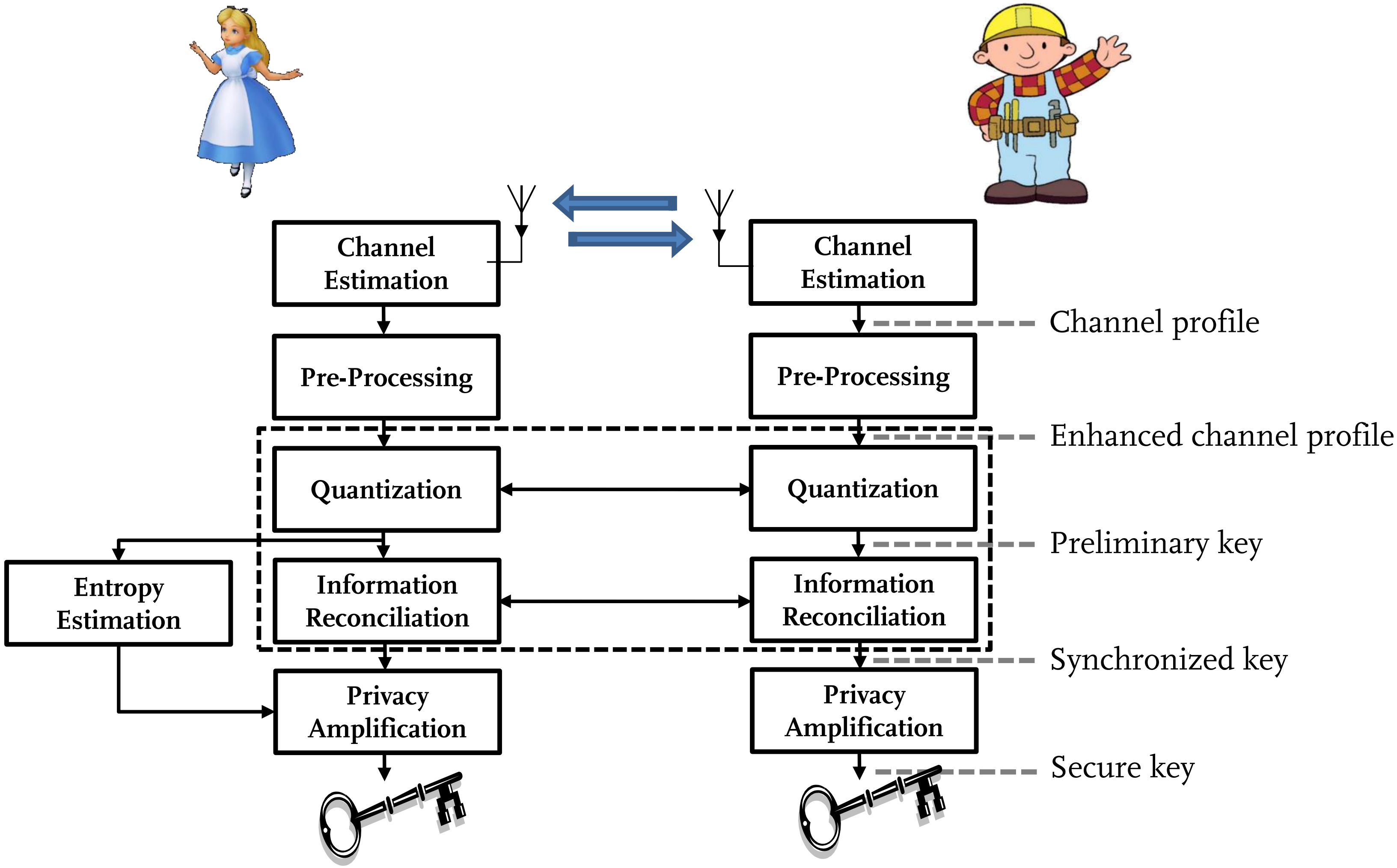
Channel Diversity



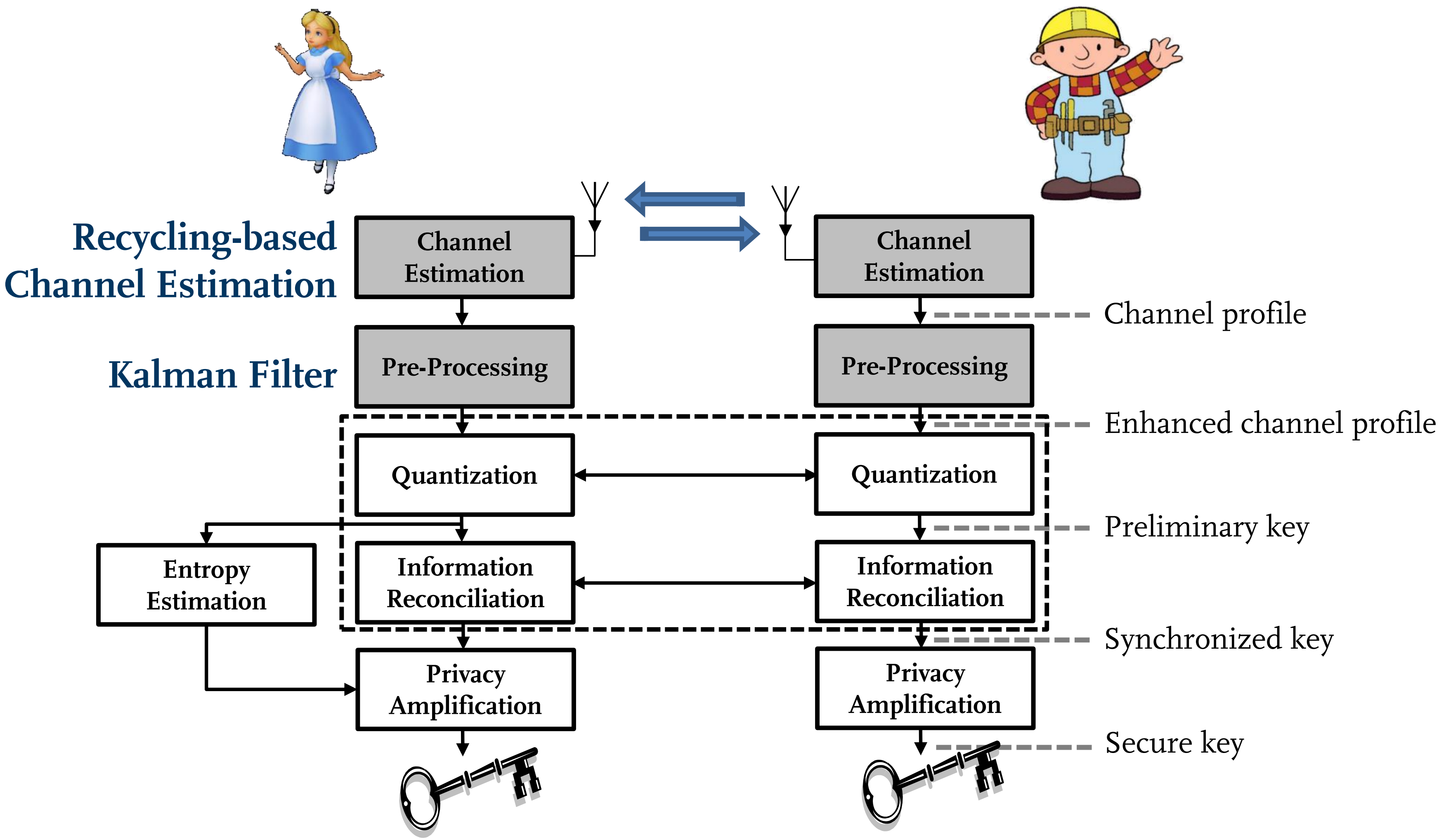
- Multipath propagation varies in space.
- Receiver at different positions estimate different channels.
- The channel decorrelates over the coherence distance $\lambda/2$.
- e.g., for a carrier frequency of 2.4 GHz $\lambda/2 = 6.25$ cm.

PHYSEC Architecture

RUB



PHYSEC Architecture

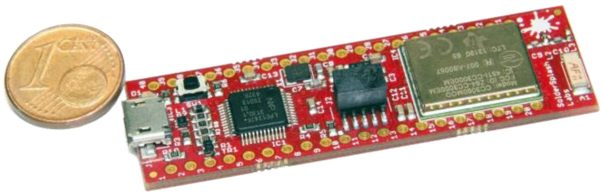


Prototype Platforms

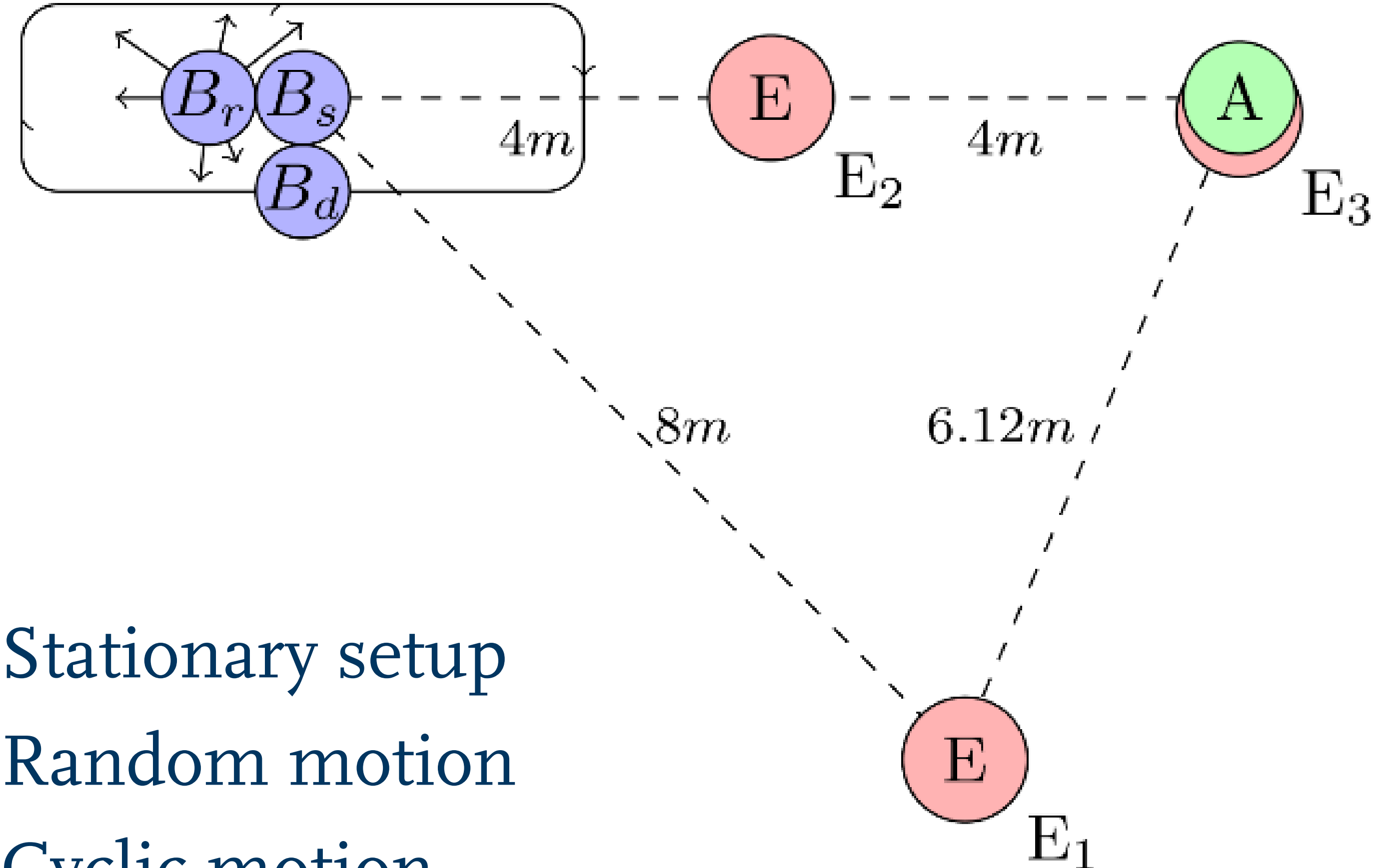
RUB

- **Alice & Eve:** Cisco Linksys WRT54gl
  - CPU BCM5352 @ 200 MHz
  - BCM2050 radio chip

- **Bob:** Wi-Fi DipCortex by Soldar Splash
  - ARM Cortex M3 @ 48 MHz
  - CC3000 radio chip

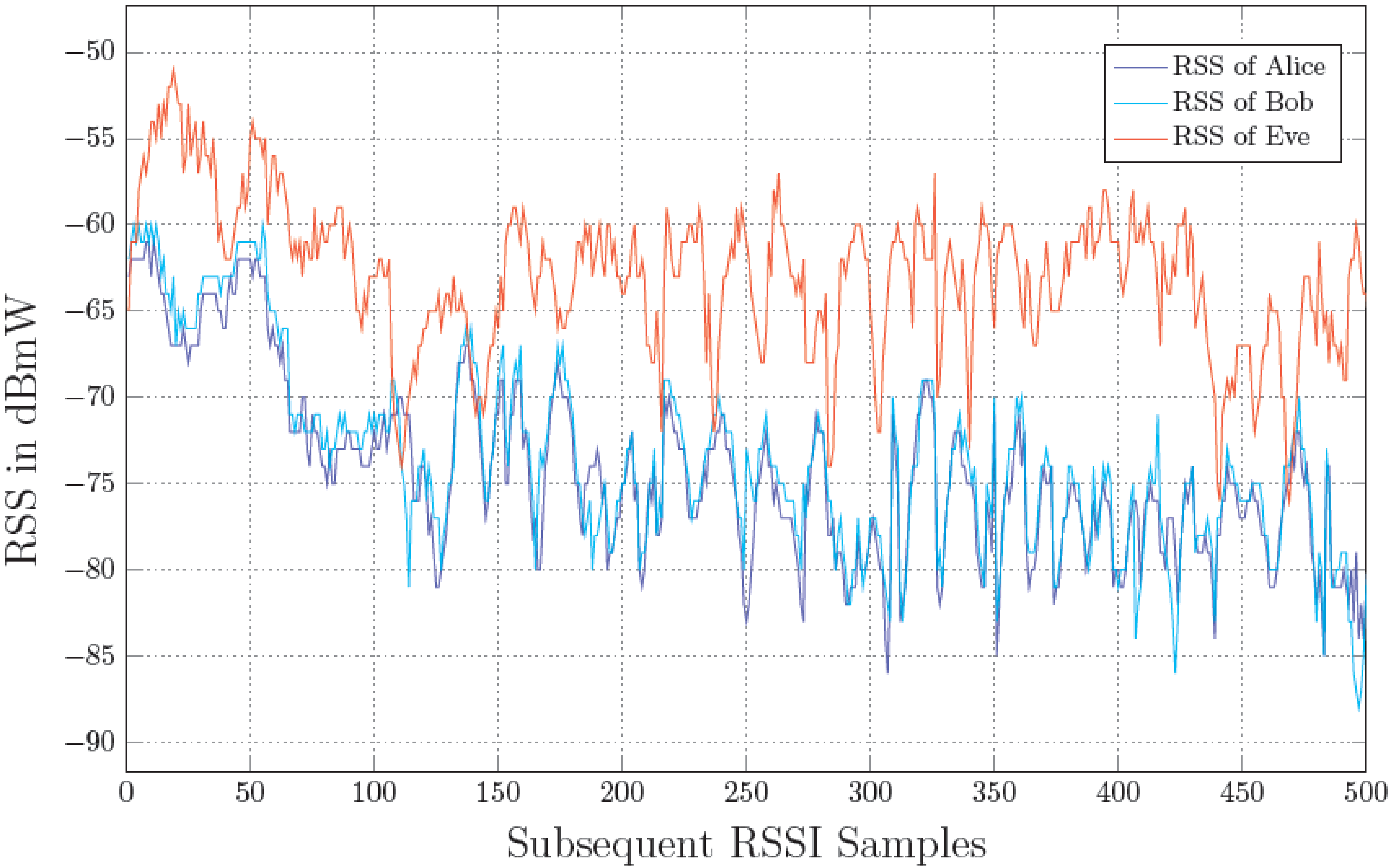


Experimental Setups



- Stationary setup
- Random motion
- Cyclic motion

Experimental Setups



Results

	Quantization schemes	Without Kalman filter BCH(n,k,d)	(#Samples)	With Kalman filter BCH(n,k,d)	(#Samples)
Stationary setup	Ambekar et al.[3]	(63,7,31)	7334	(63,7,31)	1572
	Jana et al.(SB)[31]	(63,18,21)	**2200**	(63,45,7)	**512**
	Jana et al.(MB)[31]	(63,7,31)	3143	(63,7,31)	1100
	Tope et al.[47]	(63,7,31)	5500	(63,18,21)	2445
	Aono et al.[5]	(63,7,31)	11000	(63,36,11)	2200
	Mathur et al.[33]	(63,45,7)	11000	(63,45,7)	22000
Random motion	Ambekar et al.[3]	(63,10,27)	656	(63,7,31)	**2200**
	Jana et al.(SB)[31]	(63,45,7)	**422**	(63,18,21)	**2370**
	Jana et al.(MB)[31]	(63,10,27)	670	(63,7,31)	4400
	Tope et al.[47]	(63,18,21)	1184	(63,7,31)	7700
	Aono et al.[5]	(63,36,11)	717	(63,7,31)	4400
	Mathur et al.[33]	(63,45,7)	7700	-	-
Cyclic motion	Ambekar et al.[3]	(63,10,27)	642	(63,7,31)	1340
	Jana et al.(SB)[31]	(63,45,7)	**347**	(63,36,11)	**642**
	Jana et al.(MB)[31]	(63,10,27)	604	(63,7,31)	1063
	Tope et al.[47]	(63,18,21)	1184	(63,7,31)	3080
	Aono et al.[5]	(63,30,13)	550	(63,10,27)	1467
	Mathur et al.[33]	(63,45,7)	5134	(63,45,7)	3423

Results

RUB

	Quantization schemes	Without Kalman filter BCH(n,k,d)	Without Kalman filter (#Samples)	With Kalman filter BCH(n,k,d)	With Kalman filter (#Samples)
Stationary setup	Ambekar et al.[3]	(63,7,31)	7334	(63,7,31)	1572
	Jana et al.(SB)[31]	(63,18,21)	**2200**	(63,45,7)	**512**
	Jana et al.(MB)[31]	(63,7,31)	3143	(63,7,31)	1100
	Tope et al.[47]	(63,7,31)	5500	(63,18,21)	2445
	Aono et al.[5]	(63,7,31)	11000	(63,36,11)	2200
	Mathur et al.[33]	(63,45,7)	11000	(63,45,7)	22000
			37 Min.		9 Min.
Random motion	Ambekar et al.[3]	(63,10,27)	656	(63,7,31)	**2200**
	Jana et al.(SB)[31]	(63,45,7)	**422**	(63,18,21)	**2370**
	Jana et al.(MB)[31]	(63,10,27)	670	(63,7,31)	4400
	Tope et al.[47]	(63,18,21)	1184	(63,7,31)	7700
	Aono et al.[5]	(63,36,11)	717	(63,7,31)	4400
	Mathur et al.[33]	(63,45,7)	7700	-	-
			7 Min.		40 Min.
Cyclic motion	Ambekar et al.[3]	(63,10,27)	642	(63,7,31)	1340
	Jana et al.(SB)[31]	(63,45,7)	**347**	(63,36,11)	**642**
	Jana et al.(MB)[31]	(63,10,27)	604	(63,7,31)	1063
	Tope et al.[47]	(63,18,21)	1184	(63,7,31)	3080
	Aono et al.[5]	(63,30,13)	550	(63,10,27)	1467
	Mathur et al.[33]	(63,45,7)	5134	(63,45,7)	3423
			6 Min.		11 Min.

Results & Intermediate Conclusion

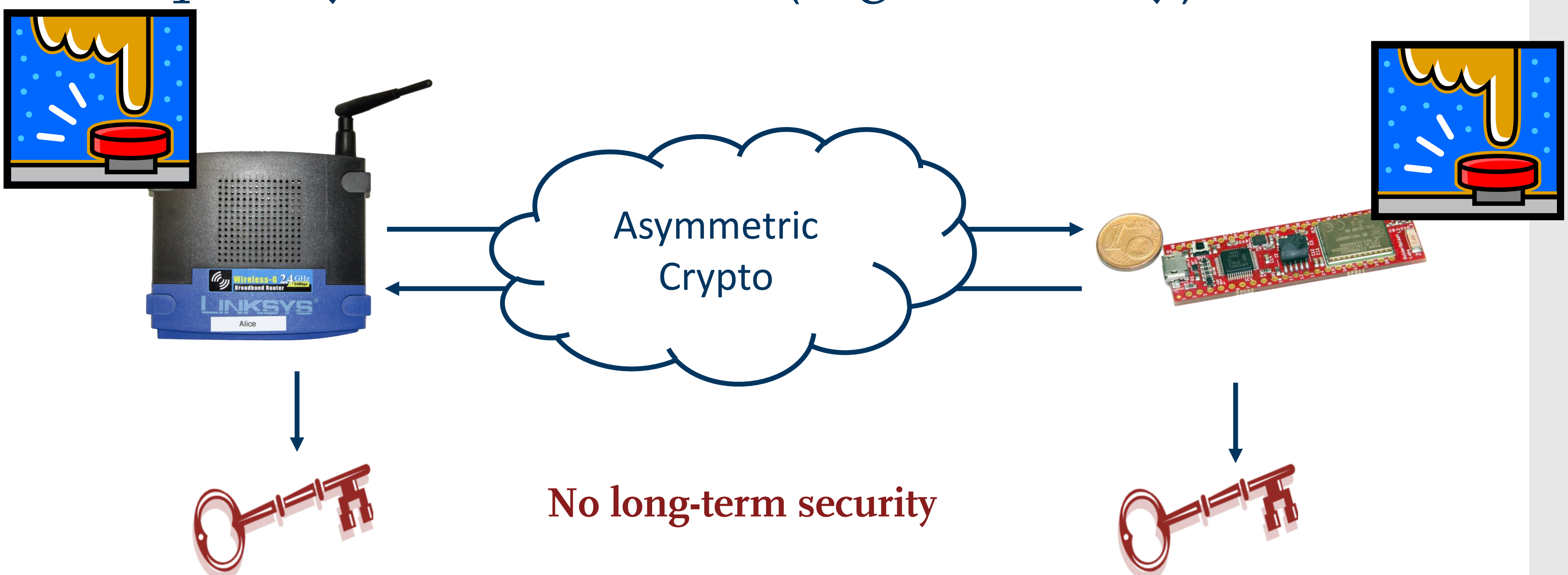
- The key generation time mainly depends on setup:
  - Very best case: 128 bit key within **6 minutes**
  - Worst case: 128 bit key after **8 hours**

- Key generation is too time intensive for time-sensitive systems (or impatient users)

- Idea:
  - **Hybrid security architecture!**

Two Stage Hybrid Approach

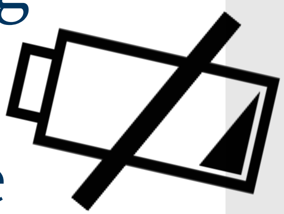
- **Stage 1:** performing a short-term authentication using asymmetric crypto (e.g., ECC sect131r1)
  - Energy efficient (cubic complexity)
  - quickly establishment (high usability)

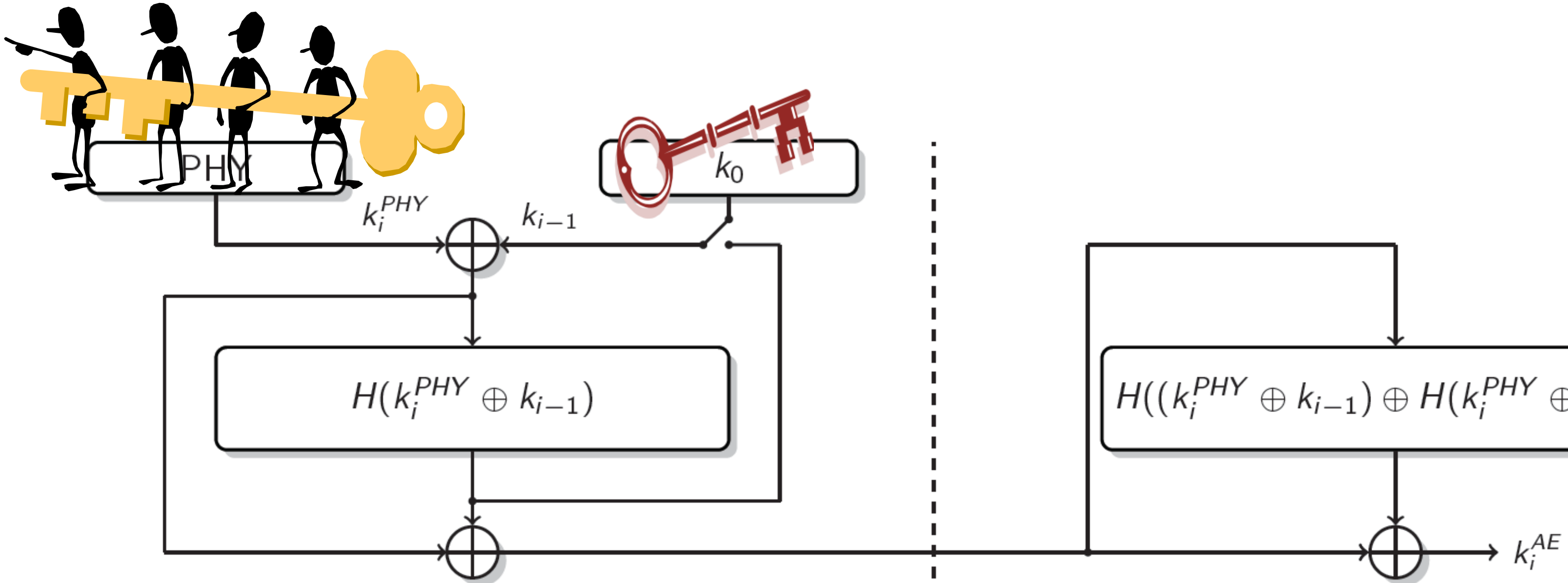


Two Stage Hybrid Approach

RUB

- **Stage 2:** The short-term key is then amplified into a long-term (and secure) symmetric key using PHYSEC
  - By passively salvaging channel profiles the system provides PFS highly energy efficient





Two Stage Hybrid Approach

RUB

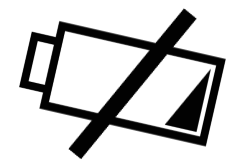
1. Usable Security: applicable for time-sensitive systems (or impatient users)

2. No scaling of attacks in time and space:
   - Perfect Forward Secrecy due to repeatedly PHYSEC-key generation
   - Key diversity due to channel charateristics

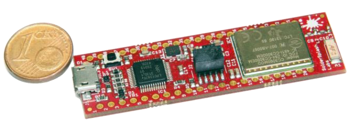
3. Energy efficient due to passively salvaging channel profiles -> IoT-capable

Conclusion

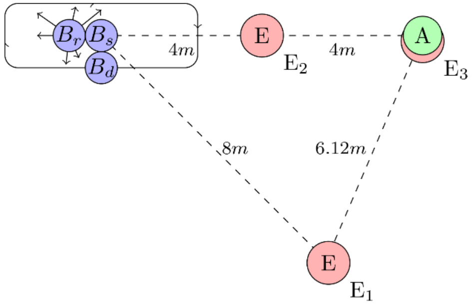
- Hybrid security architecture
  - Using asymmetric crypto to quickly establish an ephemeral short key (not long-term secure)
  - Which is then transformed into a long-term symmetric key using PHYSEC



- Prototype implementation



- Experimental security analysis and performance evaluation of different schemes [3,5,31,33,47]



RUB

Many thanks for your attention!

Questions?

… or maybe later:

christian.zenger@rub.de

hg i EMSEC

RUHR-UNIVERSITÄT BOCHUM

Lehrstuhl für Embedded Security, Prof. Dr.-Ing. C. Paar

PROPHYLAXE

Providing Physical Layer Security for the Internet of Things (PROPHYLAXE) is a strategic research project supported by the German Ministry of Education and Research. The project includes a diverse team of IT-security scientists, electrical and computer engineers and communication engineers from HGI, Fraunhofer HHI, TU-Dresden, TU-Kaiserslautern, ESCRYPT, and the BOSCH Group.

Results

RUB

- Pass rates of several NIST statistical tests for preliminary key material:

		Ambekar et al. [3]	Jana et al. [31]	Jana et al. [31] MB	Tope et al. [47]	Aono et al. [5]	Mathur et al. [33]
	# Blocks	122	37	122	30	48	1
Statistical tests	Frequency	0.77444	0.62162	0.03279	0.73333	0.87500	1.00000
	Block Frequency	0.83459	0.94595	0.00820	0.86667	0.91667	1.00000
	Cum. Sums (fwd)	0.76692	0.70270	0.01639	0.73333	0.91667	1.00000
	Cum. Sums (rev)	0.78195	0.70270	0.03279	0.73333	0.91667	1.00000
	Runs	0.71429	0.18919	0.00000	0.43333	0.41667	1.00000
	Longest Run	0.74436	0.45946	0.05738	0.63333	0.79167	1.00000
	FFT	0.82707	0.89189	0.94262	1.00000	0.97917	1.00000
	App. Entropy	0.91729	1.00000	1.00000	1.00000	1.00000	1.00000
	Serial (1)	0.65414	0.94595	0.48361	0.73333	0.93750	1.00000
	Serial (2)	0.78947	0.97297	0.67213	0.83333	0.97917	1.00000
	Linear Complexity	0.78195	0.91892	0.94262	0.93333	0.95833	0.00000