IEEE INFOCOM

ChirpKey: A Chirp-level Information-based Key Generation Scheme for LoRa Networks via Perturbed Compressed Sensing

Huanqi Yang[1], Zehua Sun[1], Hongbo Liu[2], Xianjin Xia[3], Yu Zhang[4], Tao Gu[4], Gerhard Hancke[1] , Weitao Xu[1]

[1]City University of Hong Kong

[2]University of Electronic Science and Technology of China

[3]The Hong Kong Polytechnic University, Hong Kong

[4]Macquarie University

CityU 香港城市大學 City University of Hong Kong

UESTC 1956

MACQUARIE University

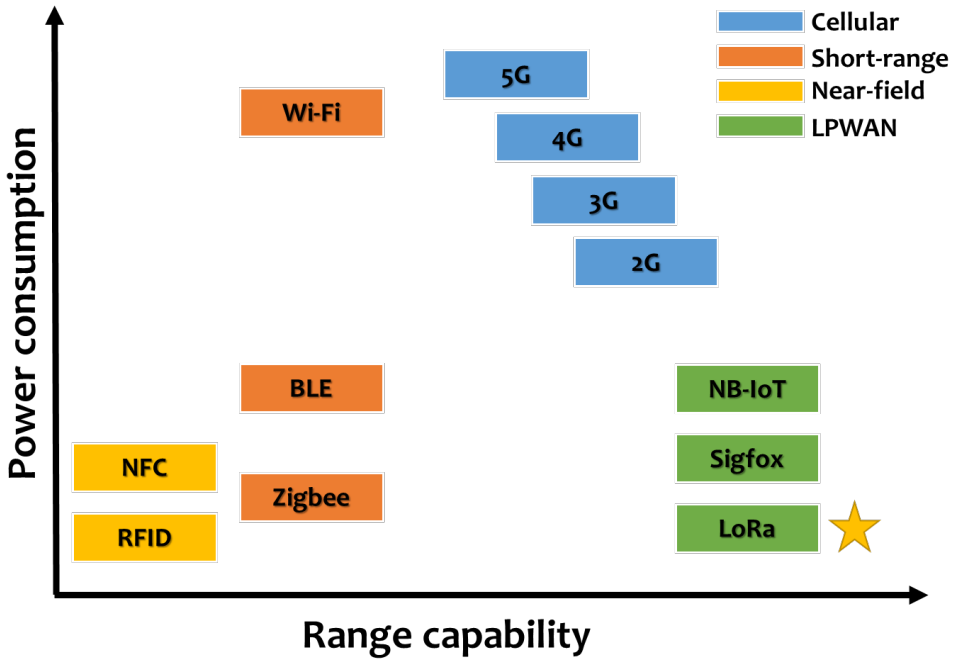
Outline

- ❑ Background
- ❑ Challenges
- ❑ Our solution
- ❑ Experiment results
- ❑ Conclusion & future work

Background

❑ Long Range (LoRa)

- ❖ One of the most representative low power wide area communication technologies
- ❖ Features low power and long range
- ❖ It is critical to ensure secure communications



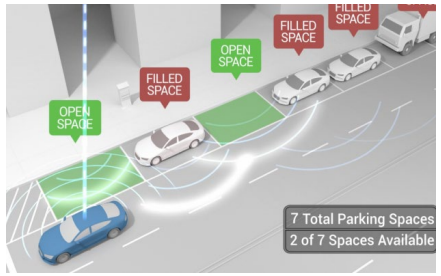
Comparison of communication technologies

Urban smart grid

Street light

Smart metering

Smart parking

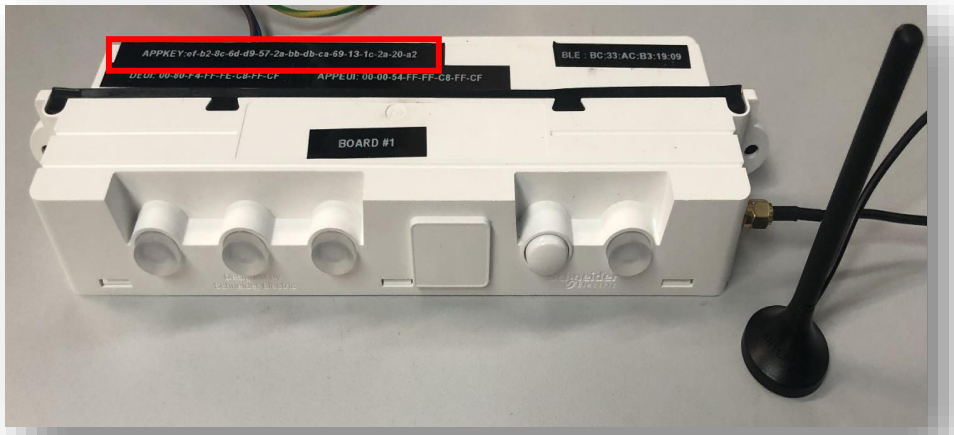


LoRa applications

Background

❑ Pre-shared key in LoRa

- ❖ Used to encrypt and decrypt messages between the end device and the network server
- ❖ Not flexible, scalable, and can be easily stolen by malicious attackers

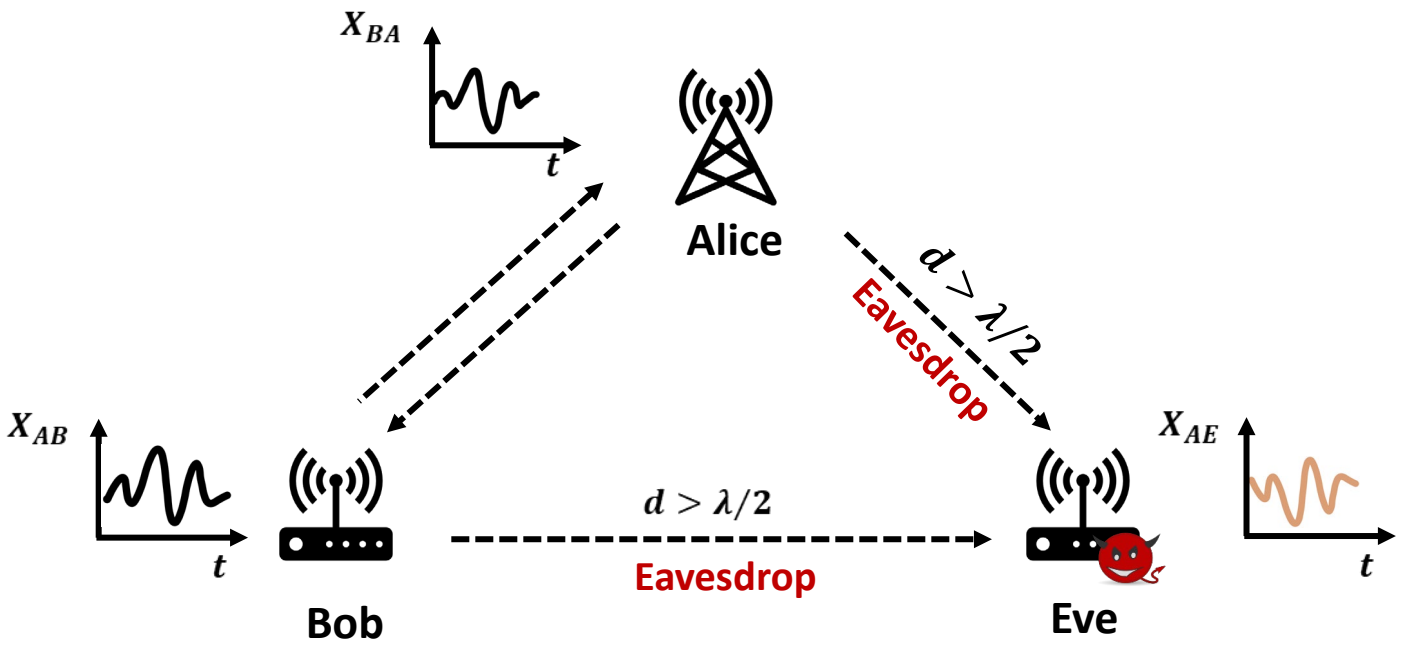


Pre-shared key in LoRa

Background

❑ Physical-layer key in LoRa

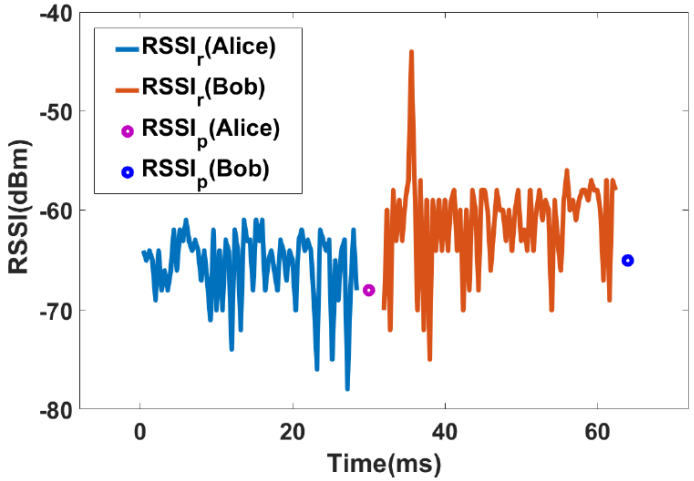
- ❖ Extract randomness from wireless channel based on **channel reciprocity**
- ❖ Existing methods are still **inefficient and unstable** due to low data rate of LoRa



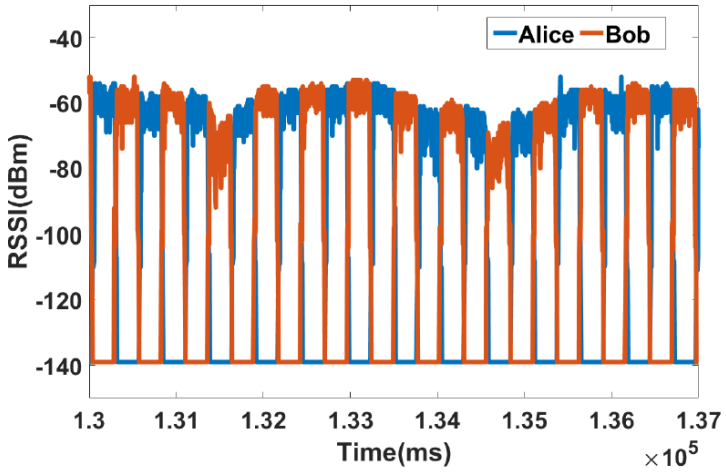
Physical-layer key in LoRa

Challenges

- **Coarse-grained and noisy channel measurement**
  - Packet RSSI ($RSSI_p$) provides **coarse-grained** channel information
  - Register RSSI ($RSSI_r$) attempts to improve granularity but still **noisy**



$RSSI_p$ and $RSSI_r$

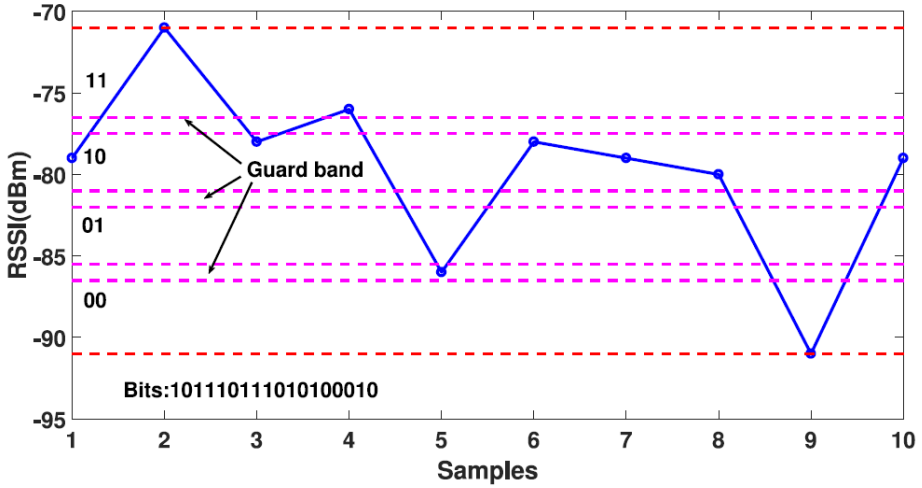


$RSSI_r$ of Alice and Bob

Resulting in impaired channel reciprocity

Challenges

- **Inefficient quantization process**
  - **Lossy and error-prone** conversion of channel measurements into binary bits
  - Increased packet exchanges

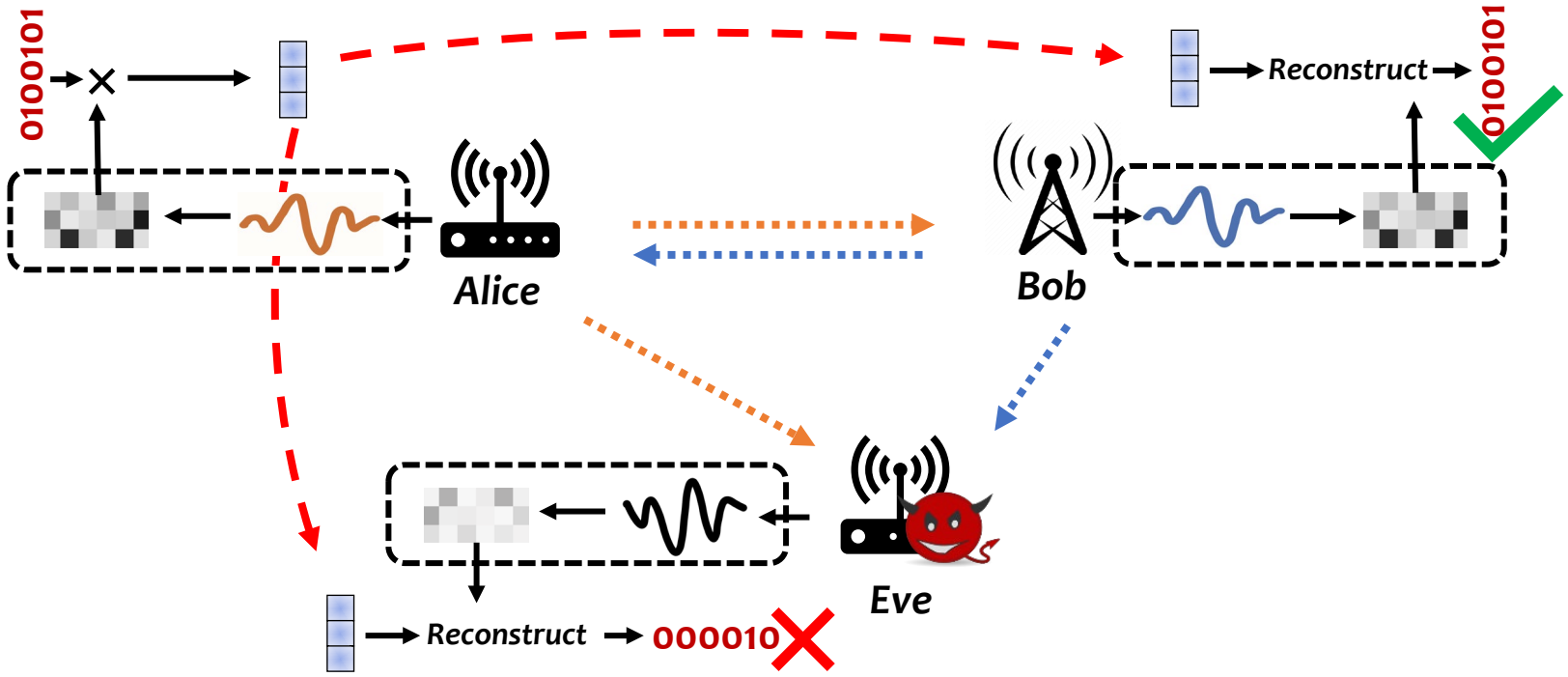


Lossy and error-prone quantization process

Resulting in system inefficiency and lack of robustness

Our solution

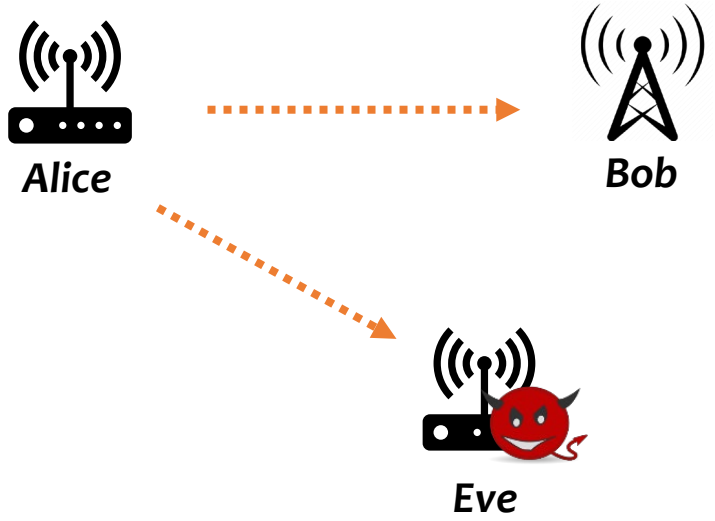
- **ChirpKey—A Chirp-level Information-based Key Generation Scheme for LoRa Networks via Perturbed Compressed Sensing**
  - LoRa-specific chirp-level channel measurement
  - Perturbed compressed sensing based key delivery method



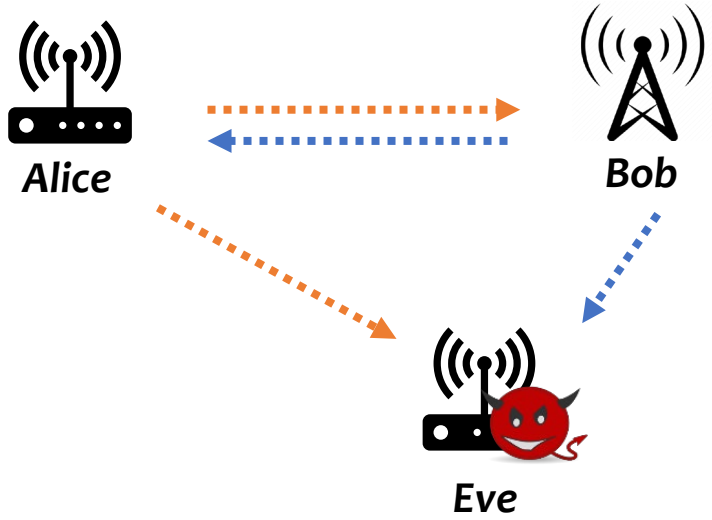
ChirpKey overview

System overview

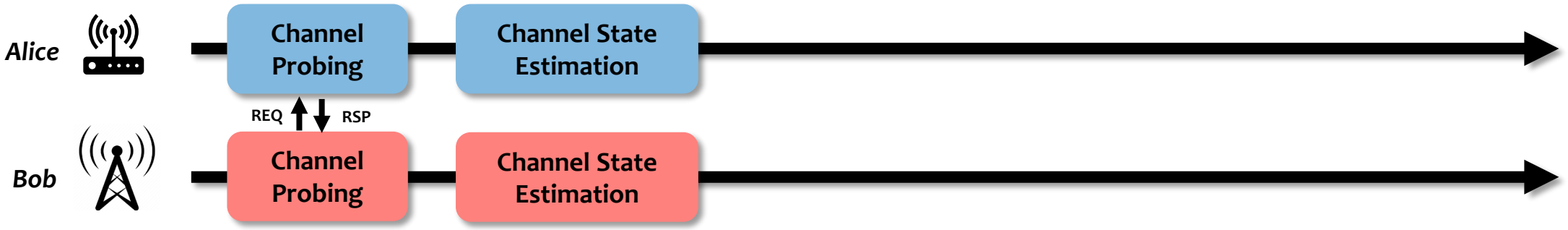
System overview

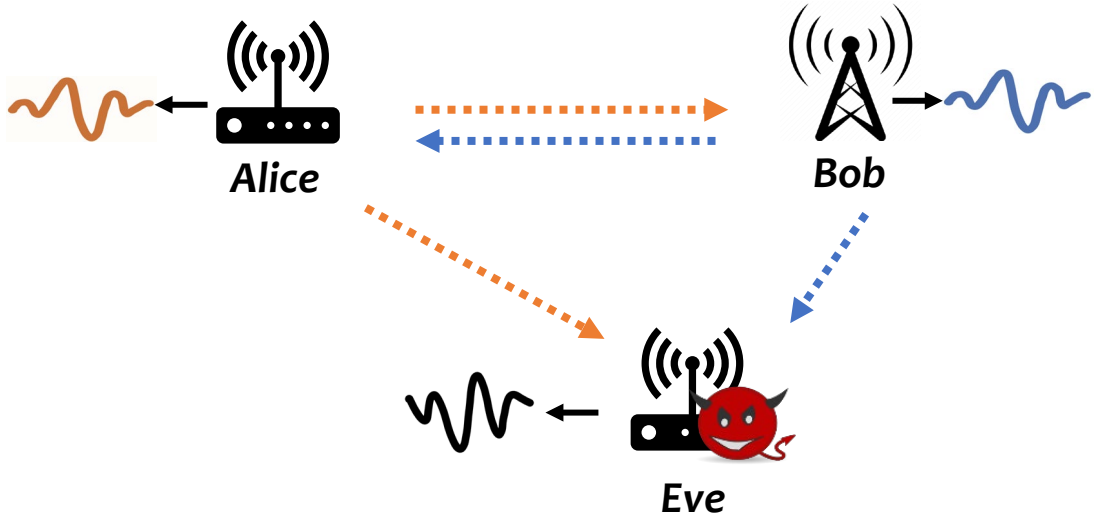


System overview

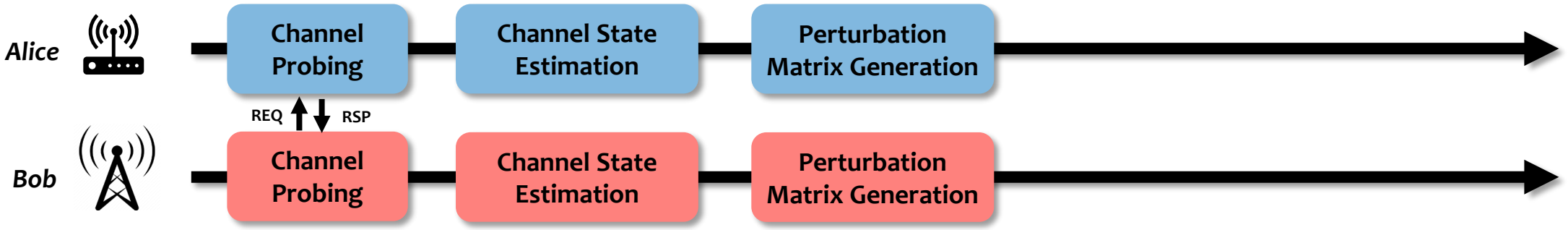


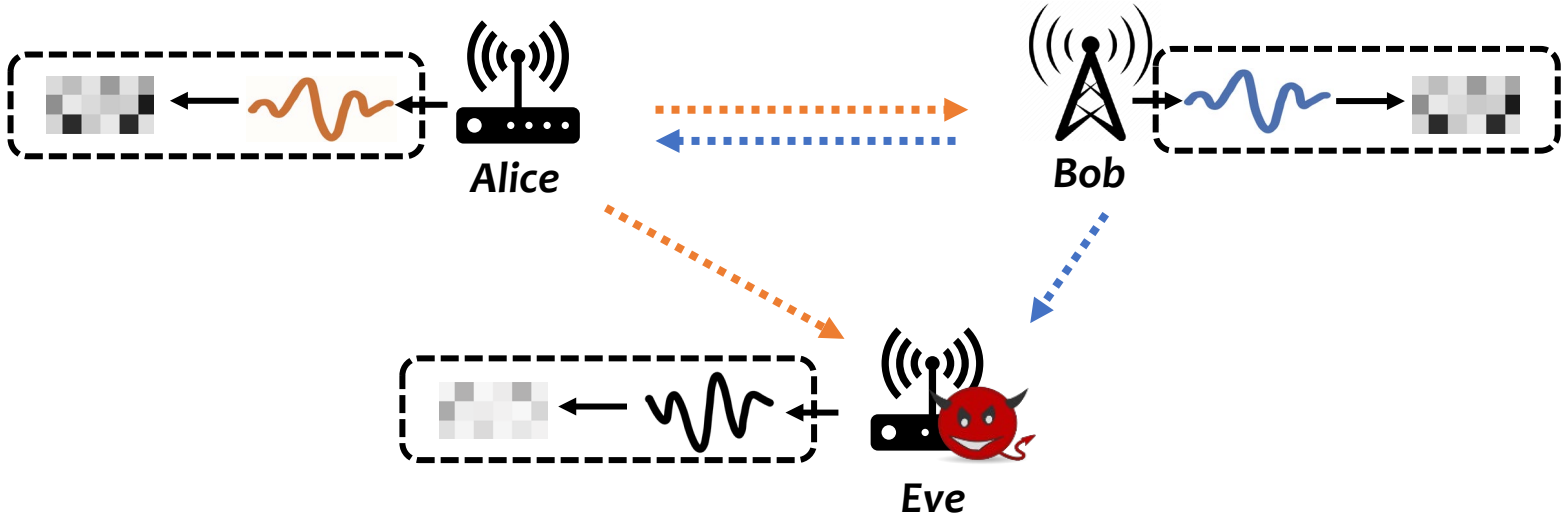
System overview



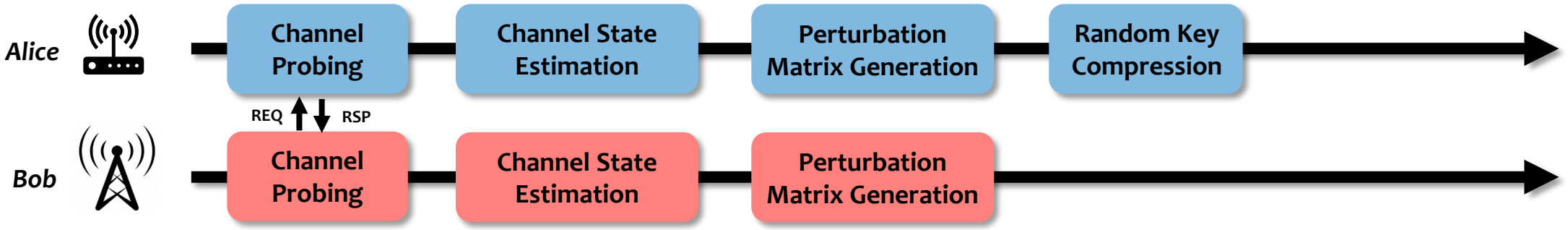


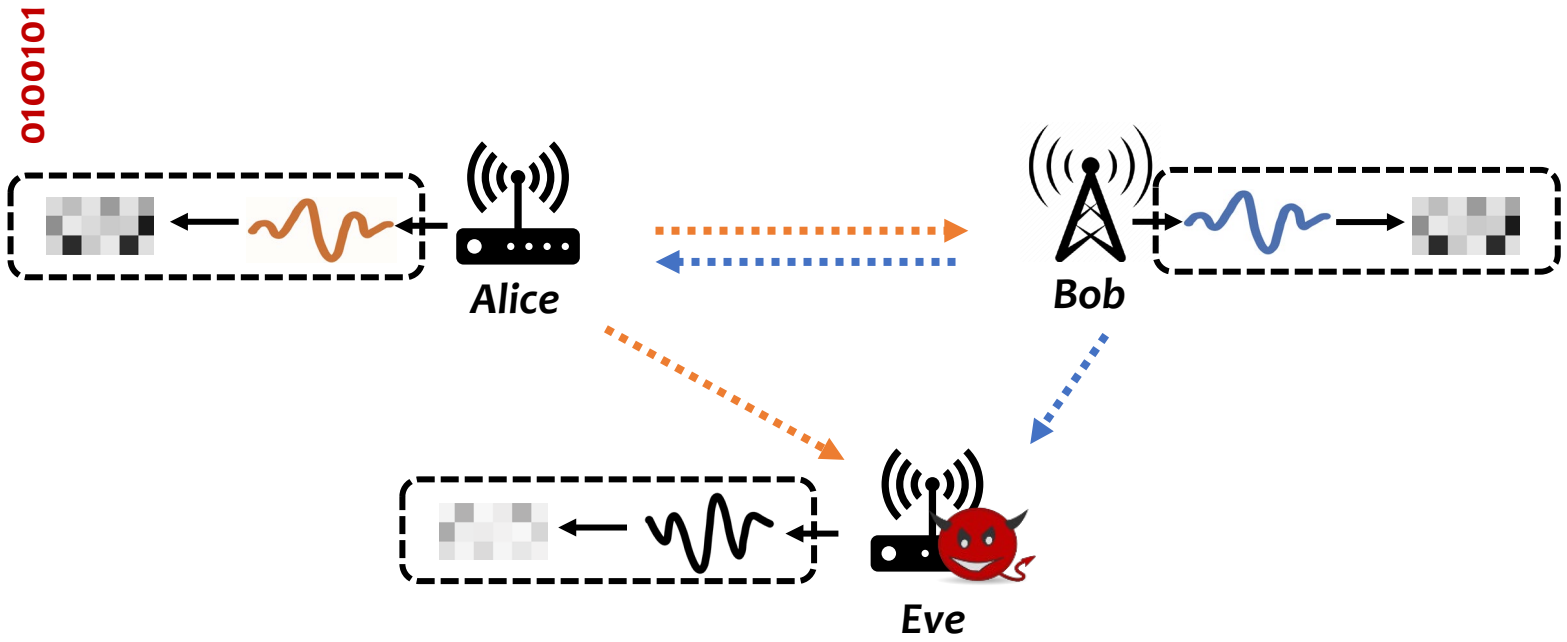
System overview



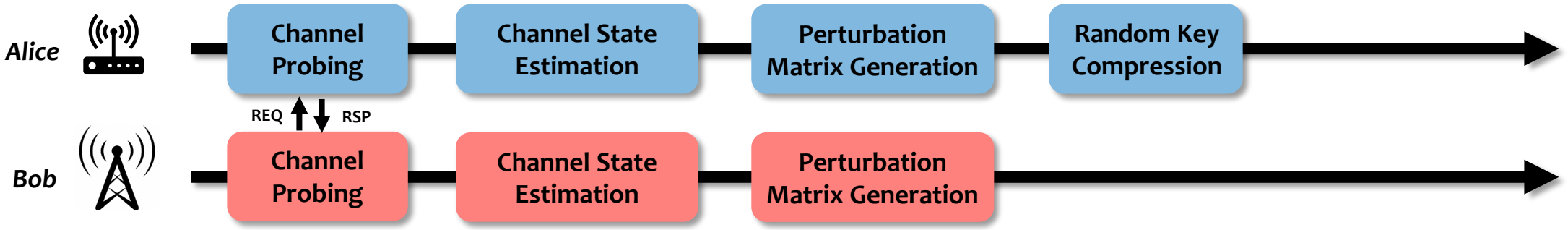


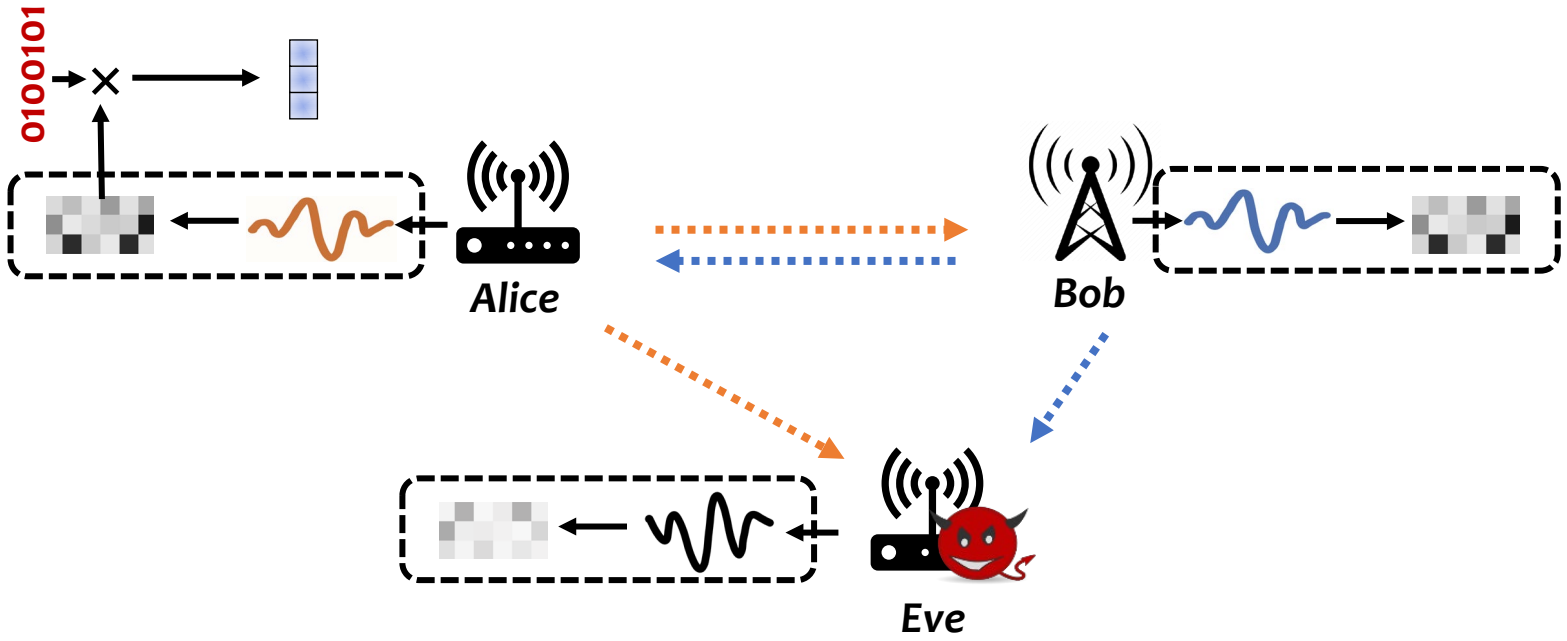
System overview



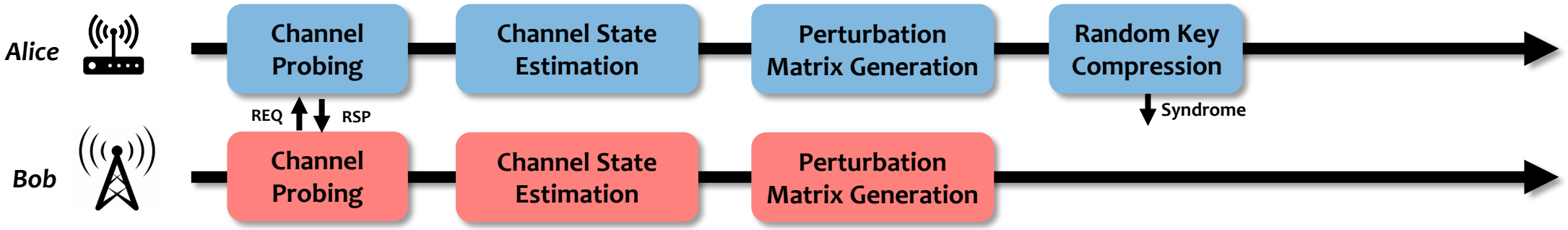


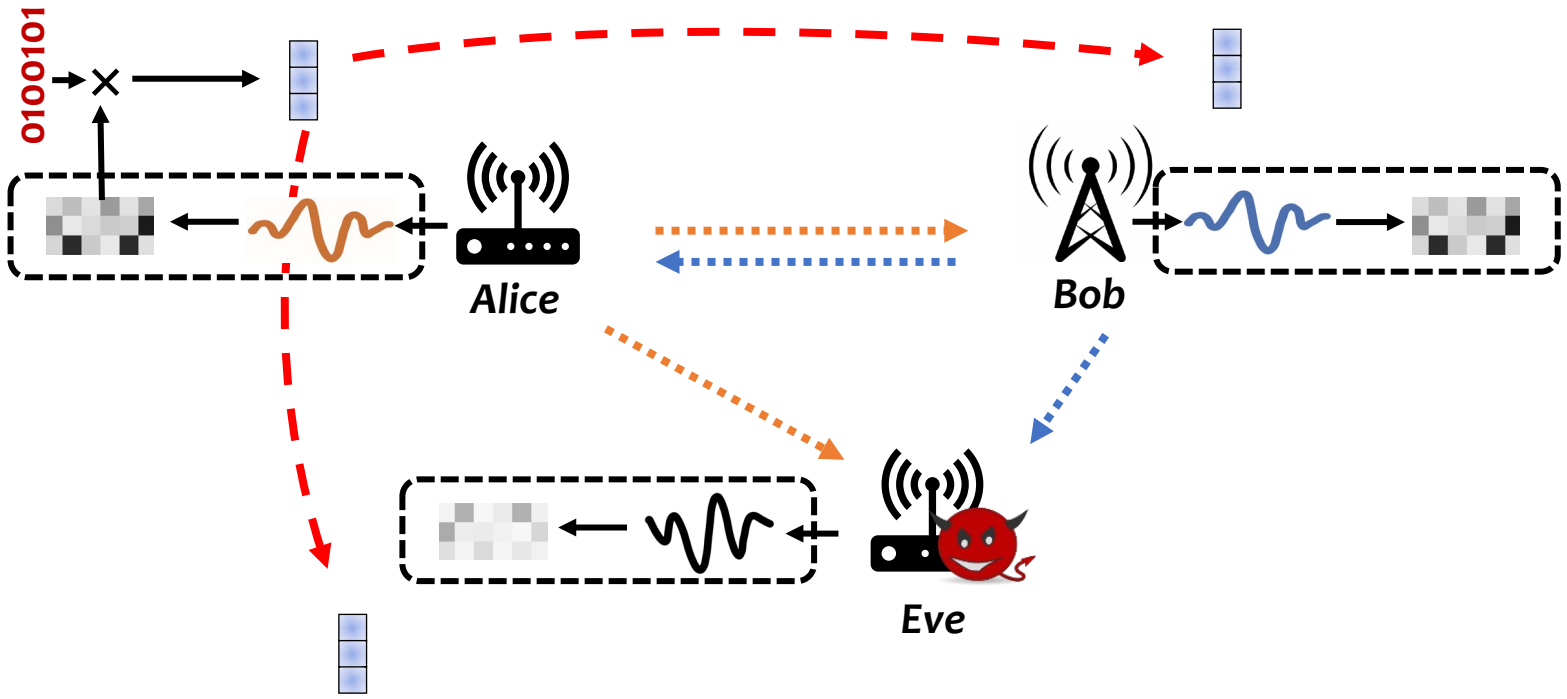
System overview



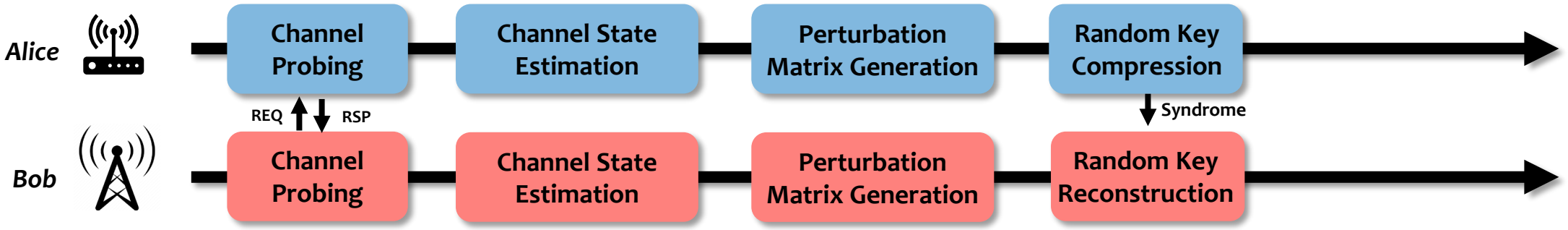


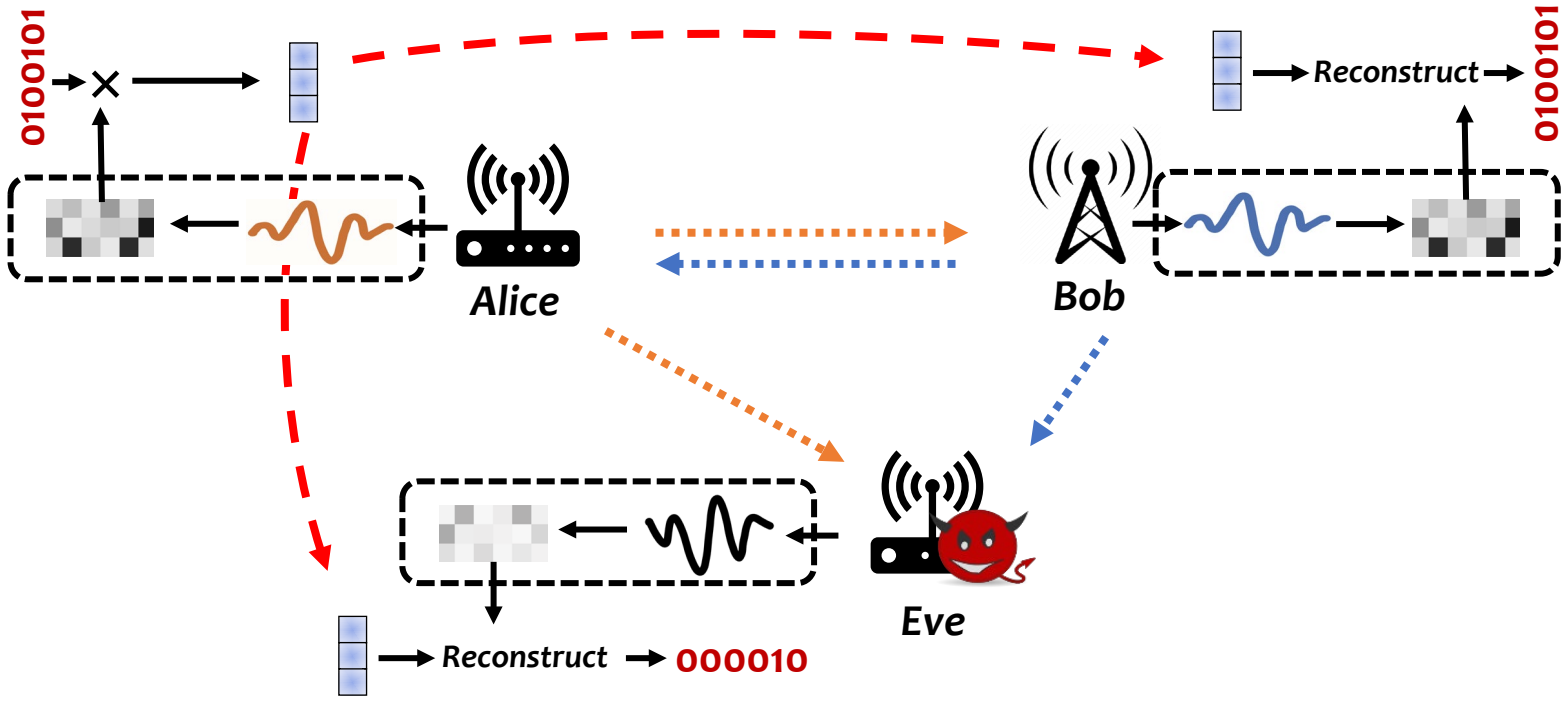
System overview



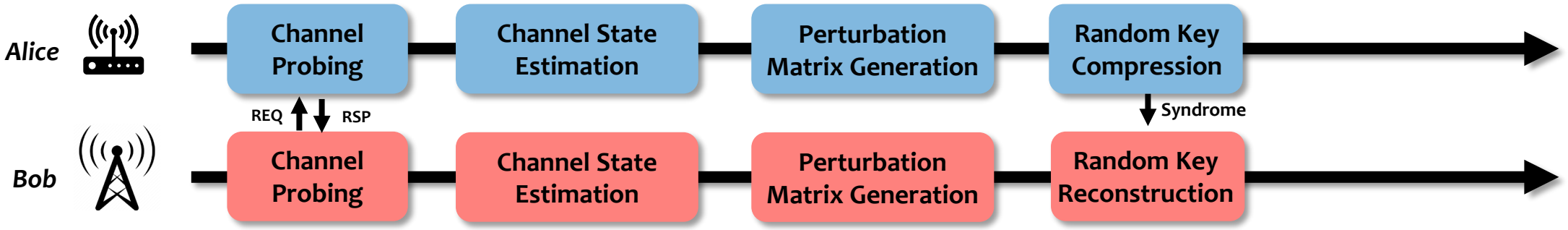


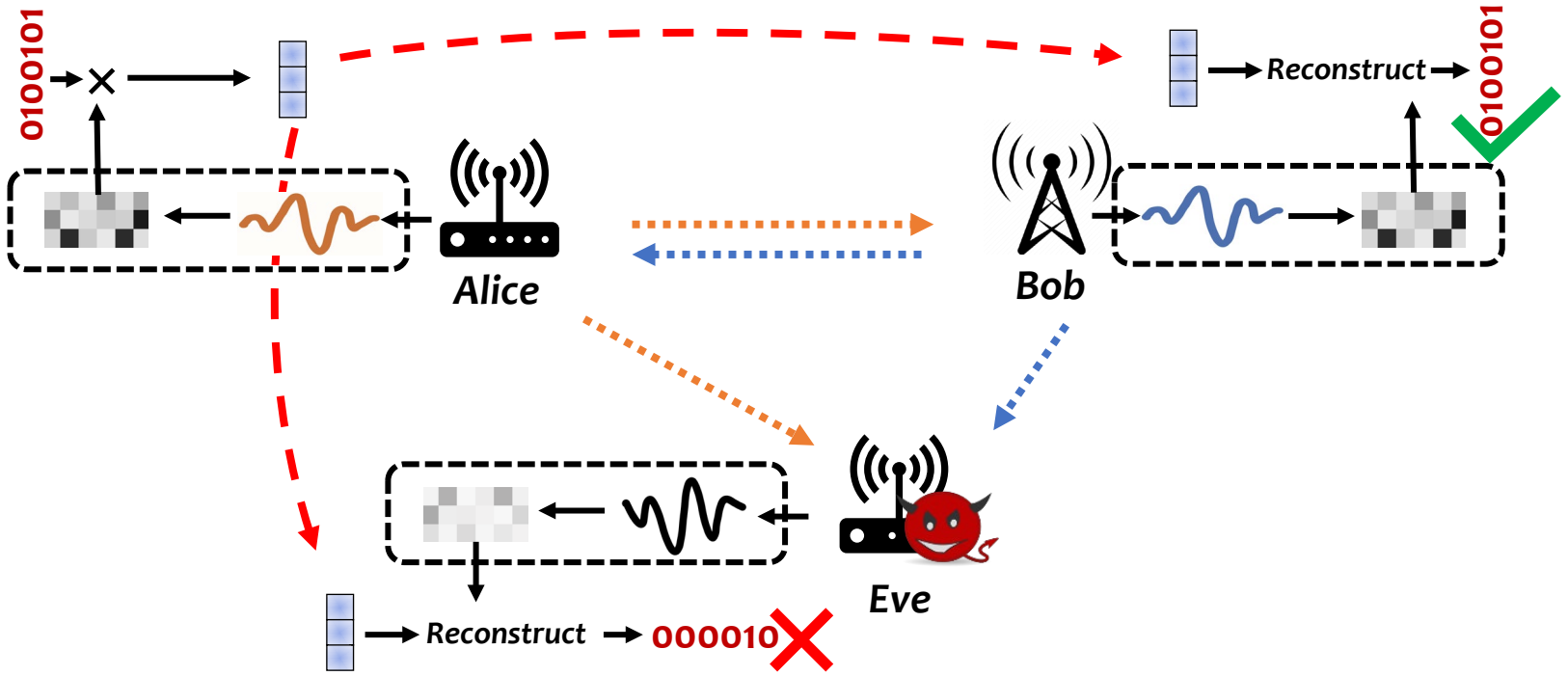
System overview



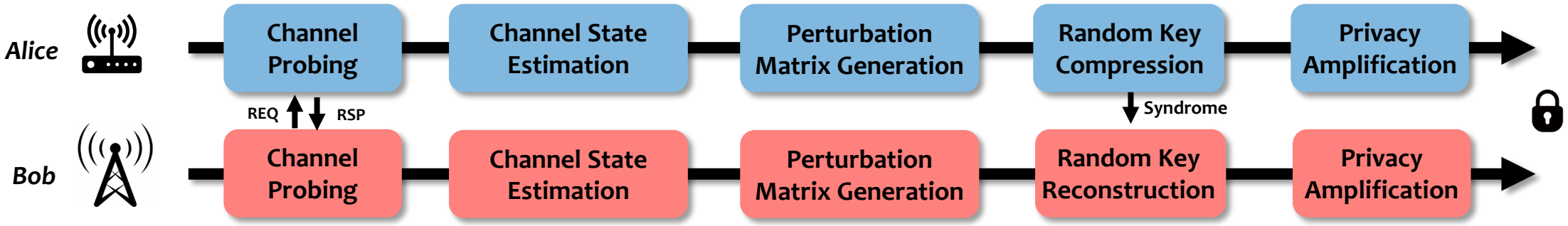


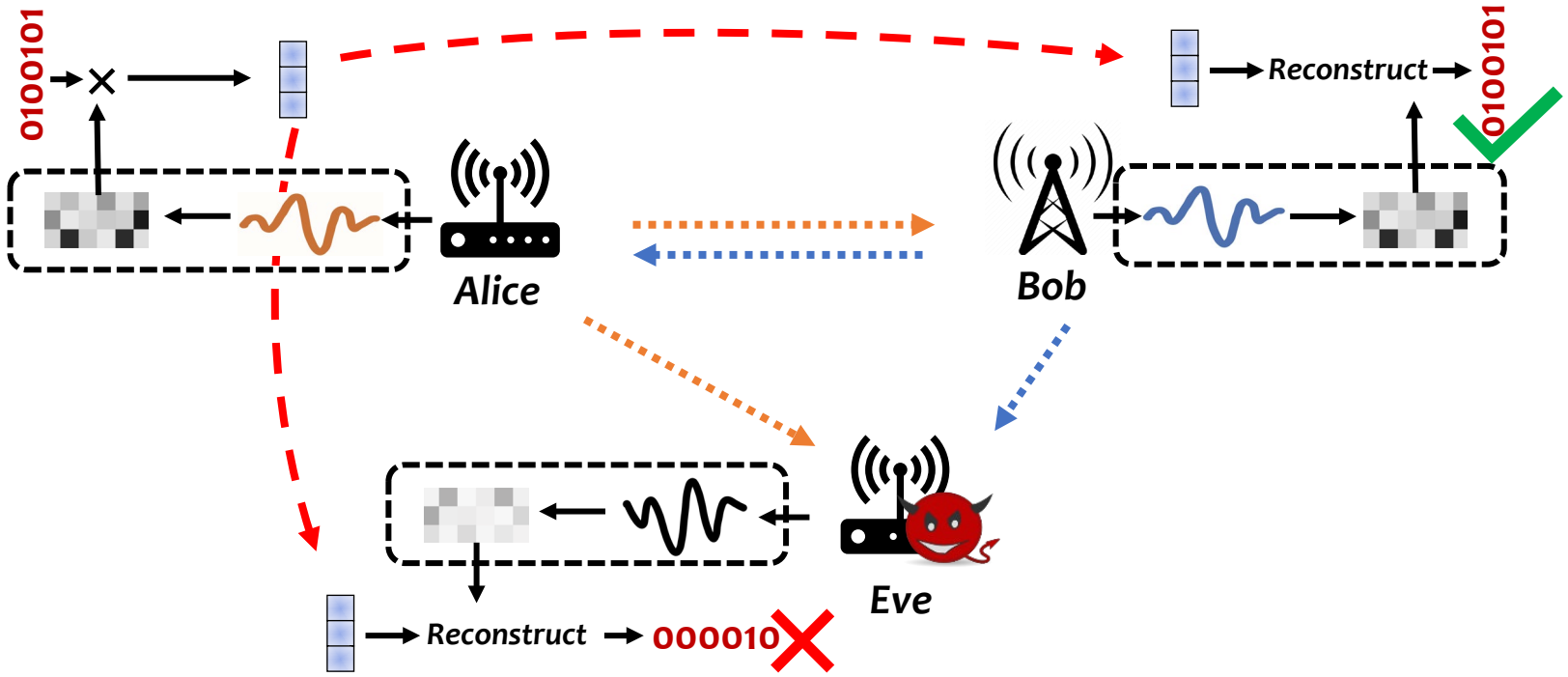
System overview





System overview

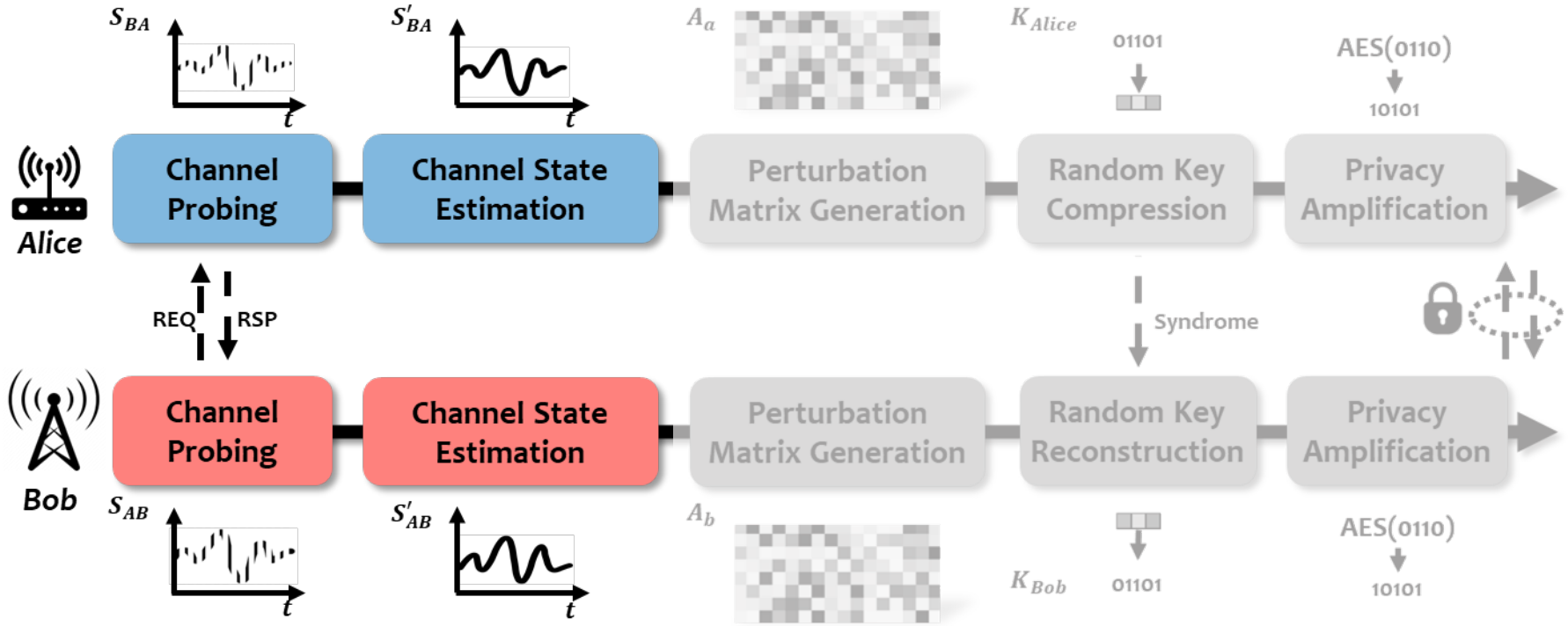




System design

❶ LoRa-specific chirp-level channel measurement

❷ Perturbed compressed sensing based key delivery method

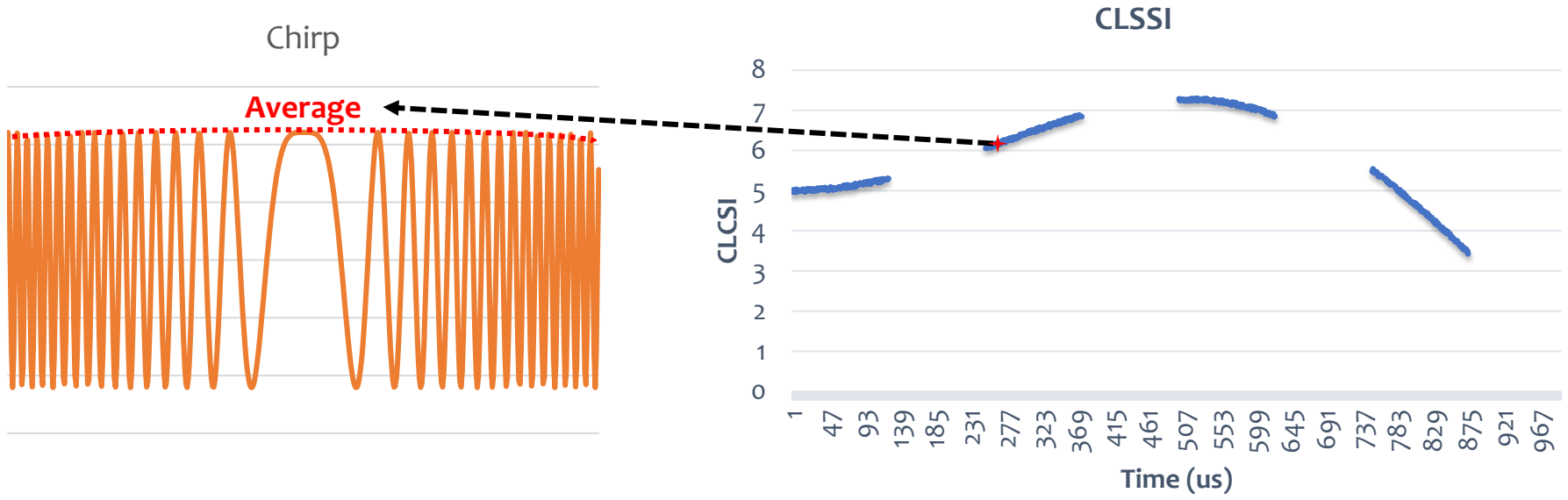


ChirpKey work-flow

System design

❑ Chirp-Level Signal Strength Indicator (CLSSI)

- ❖ A LoRa packet is composed of multiple chirps with a **constant transmitting amplitude**
- ❖ Calculate **the fine-grained changes of received chirps**
- ❖ Fine-grained chirp-level channel state indicator



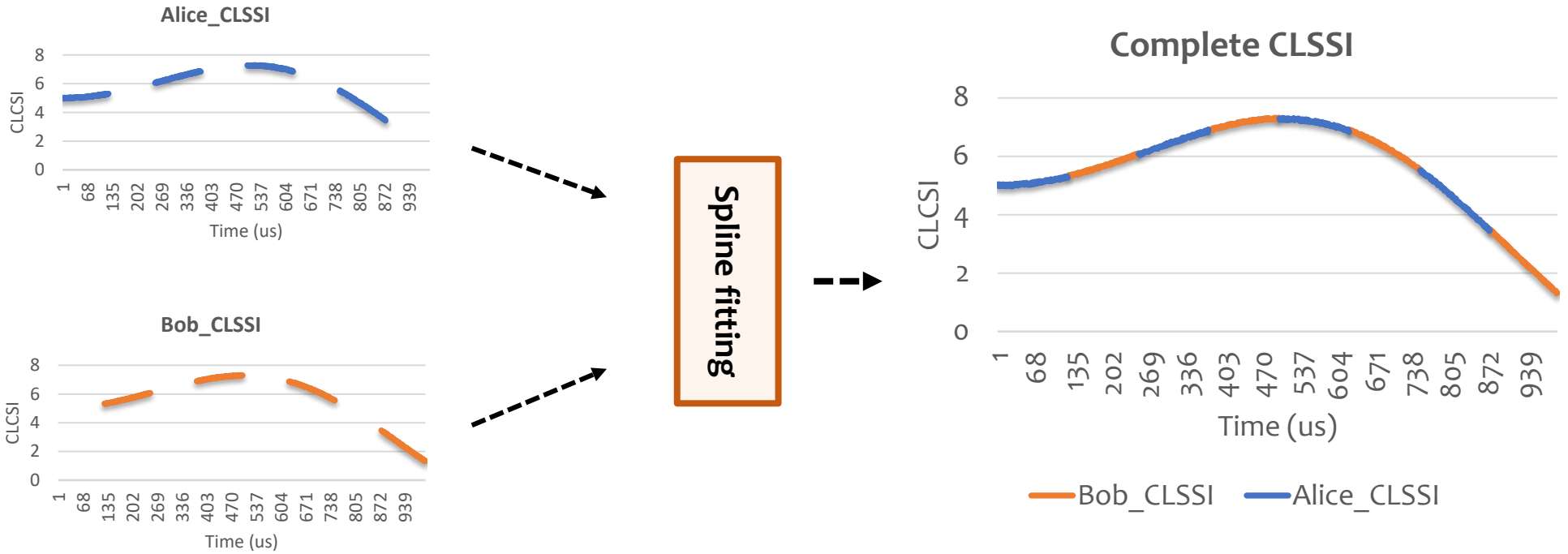
One chirp in a LoRa packet

Each CLSSI value is the average of a chirp envelop

System design

❑ Channel state estimation

- ❖ Alice and Bob send Probing packets in a **half-duplex** manner
- ❖ Complete channel information requires Alice to combine with Bob's CLSSI
- ❖ Use a lightweight **univariate spline fitting** to estimate the missing CLSSI

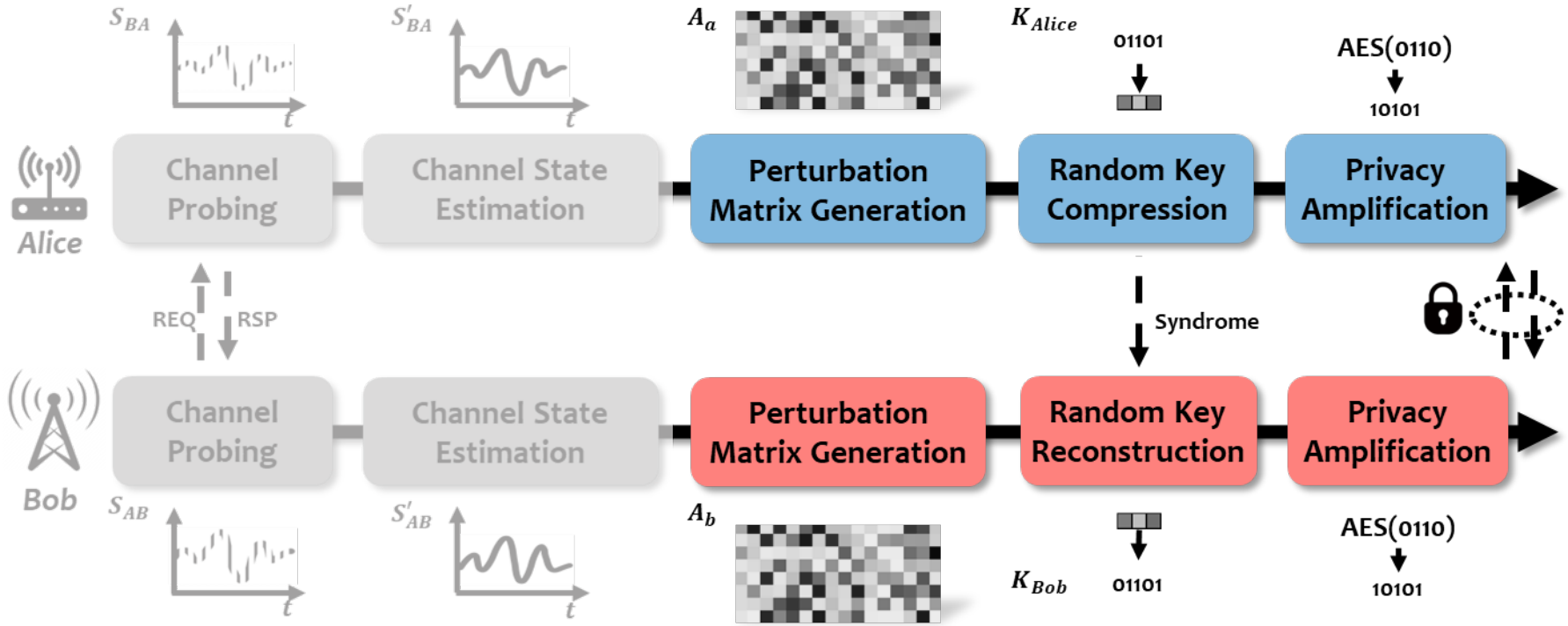


Channel State Estimation

System design

❶ LoRa-specific chirp-level channel measurement

❷ **Perturbed compressed sensing based key delivery method**



ChirpKey work-flow

System design

❑ Compressive sensing theory

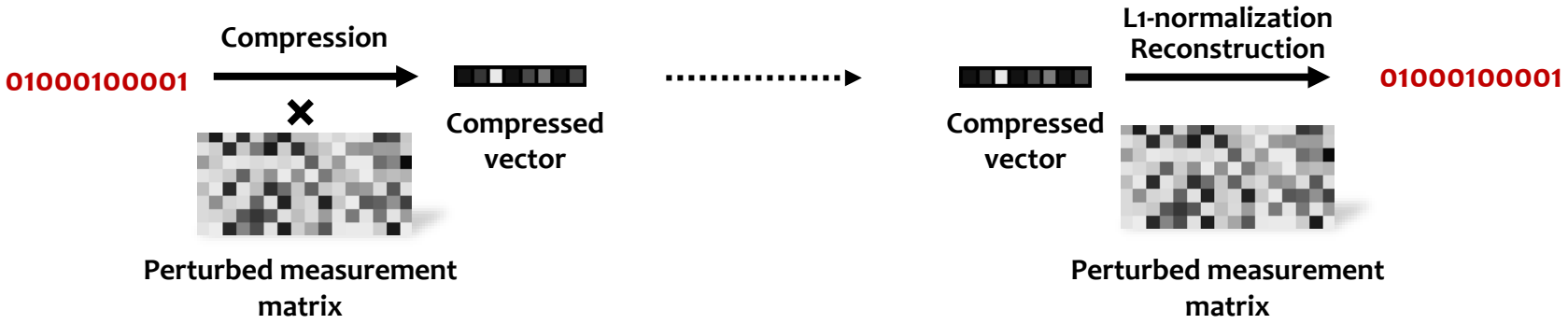
- ❖ Efficiently acquiring and reconstructing sparse signals
- ❖ Multiplying the sparse signal by a measurement matrix for **compression**
- ❖ Solving an optimization problem for **reconstruction**

Compressive sensing

System design

❑ Perturbed compressive sensing (PCS)

- ❖ Efficiently acquiring and reconstructing sparse signals with **noise tolerant ability**
- ❖ Multiplying the signal by a measurement matrix **with noise** for compression
- ❖ Solving an optimization problem for reconstruction

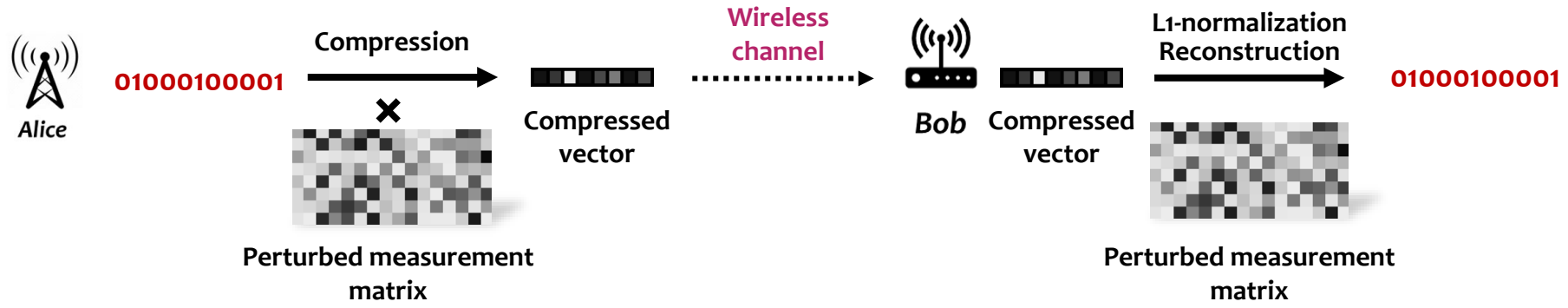


Perturbed compressive sensing

System design

❑ Perturbed compressive sensing (PCS)-based key generation

- ❖ Based on the PCS theory, the compressed key from Alice can only be reconstructed by Bob if their measurement matrices' difference is **within the noise tolerance ability for PCS**
- ❖ How to construct the perturbed measurement matrices of Alice and Bob and make their difference within the tolerance of PCS?
- ❖ **Use their similar CLSSI values to generate similar perturbed measurement matrix!**

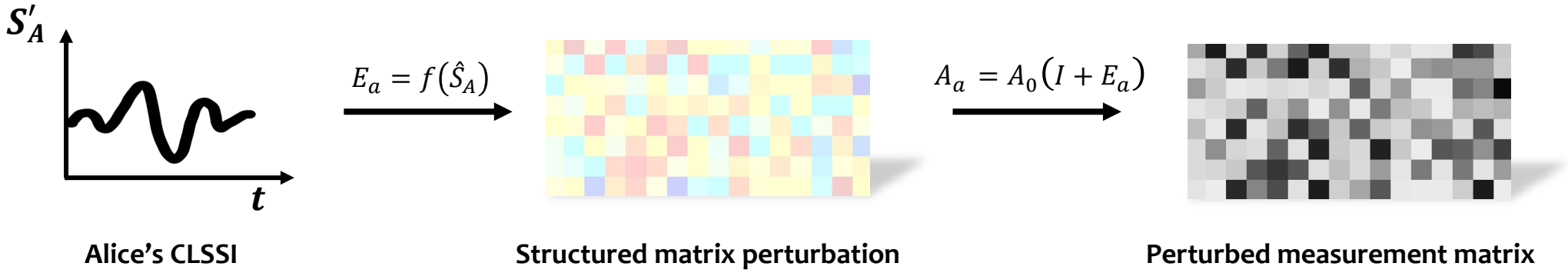


PCS-based key delivery

System design

❑ Perturbed measurement matrix generation

- ❖ Generate **default sensing matrix** A_0 (use random Gaussian matrix to generate)
- ❖ Construct $f(\hat{S}_A)$ with cyclic displacement to form **structured matrix perturbation**
- ❖ Generate **perturbed matrix** : $A_a = A_0(I + E_a)$,where I is identity matrix, and $E_a = f(\hat{S}_A)$ is generated circulant matrix

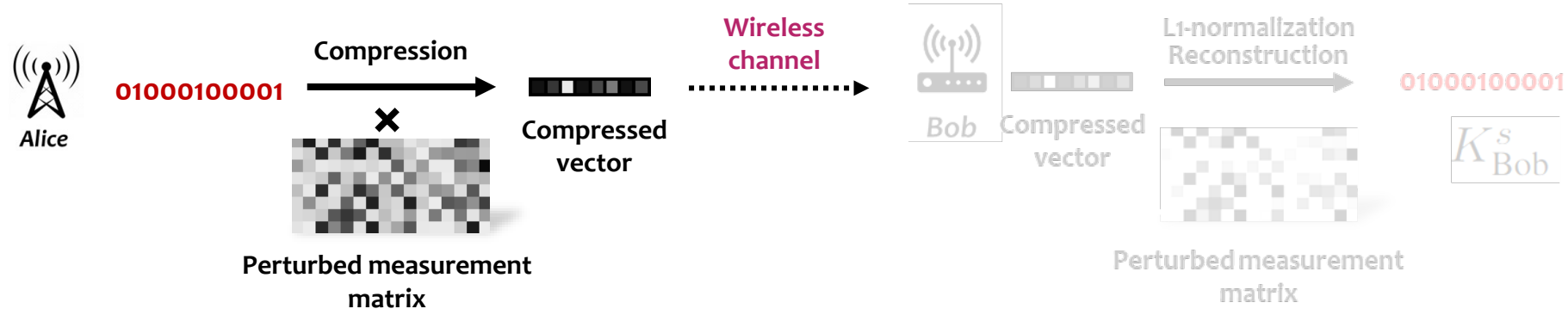


Perturbed measurement matrix generation

System design

❑ Secret key compression

- ❖ Alice generates random binary sequence
- ❖ Calculate compressed vector
- ❖ Send compressed vector through public channel to Bob

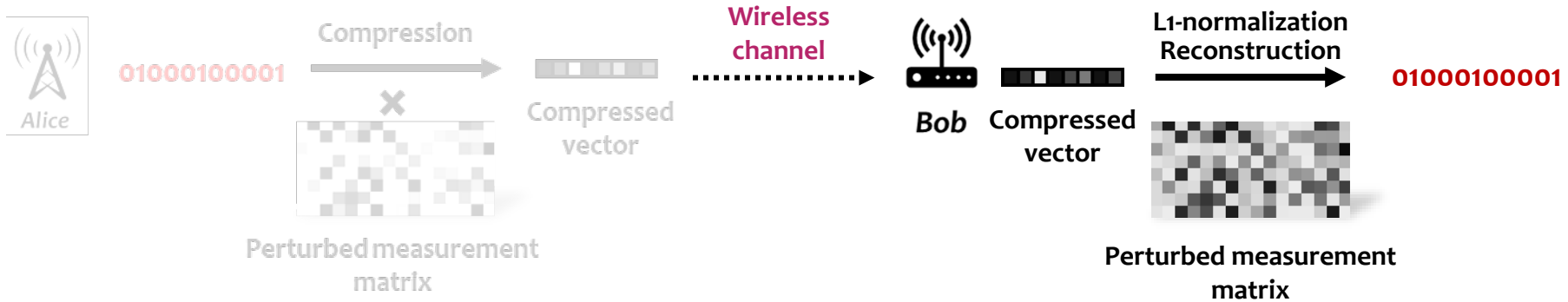


Secret key compression

System design

❑ Secret key reconstruction

- ❖ Bob receive the compressed vector
- ❖ Reconstruct the key by solving ℓ_1 -regularized total least-squares problem



Secret key reconstruction

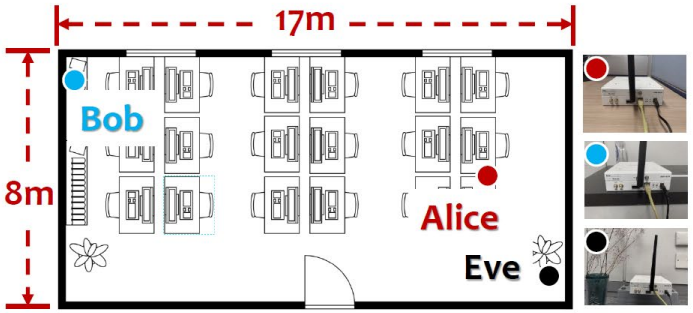
Experimental settings

❑ Data collection

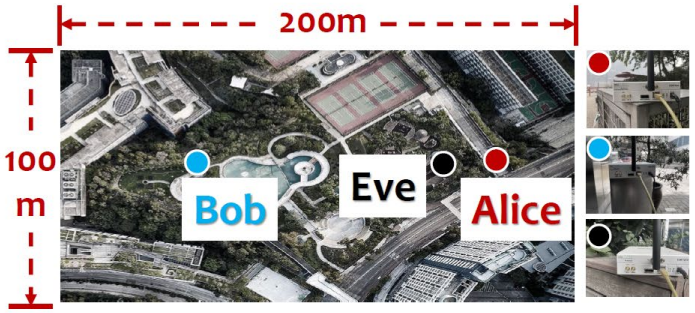
- ❖ Three USRP N210 SDR with WBX Daughterboard as Alice, Bob, and Eve
- ❖ Indoor and outdoor experiments with static and mobile node settings

❑ Metrics

- ❖ Key agreement rate: the percentage of bits matching between two keys generated by two devices
- ❖ Key generation rate: the average number of agreed keys generated from the samples per second



Indoor experiment

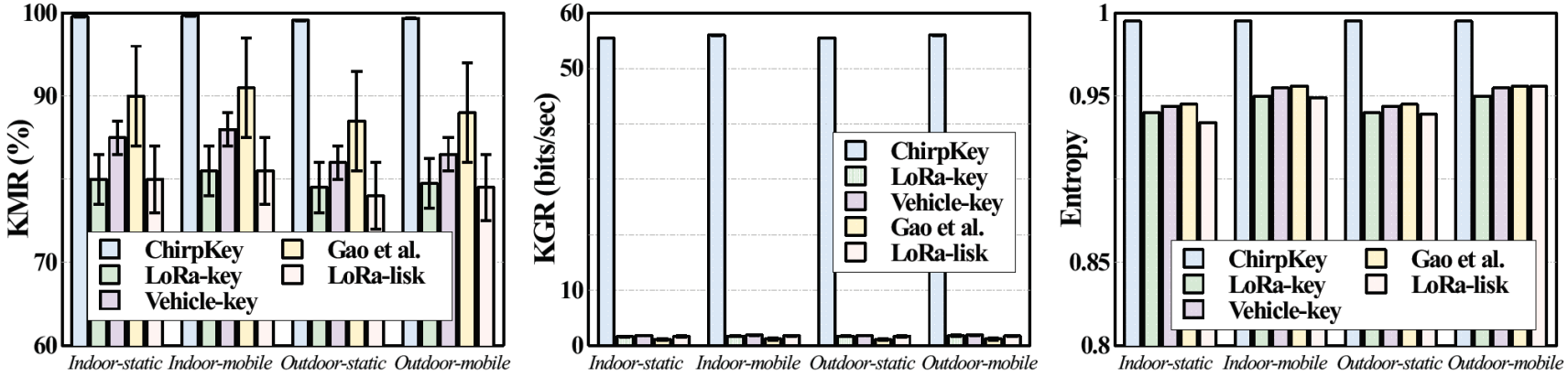


Outdoor experiment

Experiment results

❑ Comparison with state-of-the-arts

- ❖ ***LoRa-key*** uses RSSI channel measurement and compressed sensing-based reconciliation
- ❖ ***LoRa-liSK*** uses RSSI channel measurement and error correction code-based reconciliation
- ❖ ***Gao et al.*** uses register RSSI channel measurement and compressed sensing-based reconciliation
- ❖ ***Vehicle-key*** uses register RSSI channel measurement and autoencoder based reconciliation

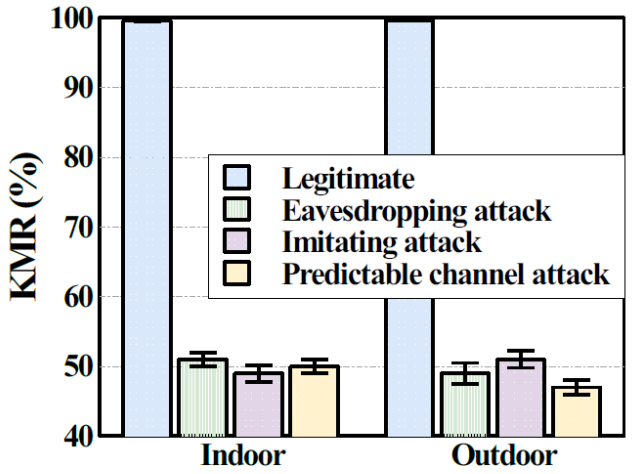


Matching rate **Generation rate** **Entropy**

Experiment results

❑ Security analysis

- ❖ Eavesdropping attack
- ❖ Imitating attack
- ❖ Predictable channel attack



Security analysis

❑ Key Randomness

- ❖ Use the NIST set of statistical tests
- ❖ P-values show the randomness level
- ❖ P-value>0.1 indicate high randomness

TABLE II: NIST test.

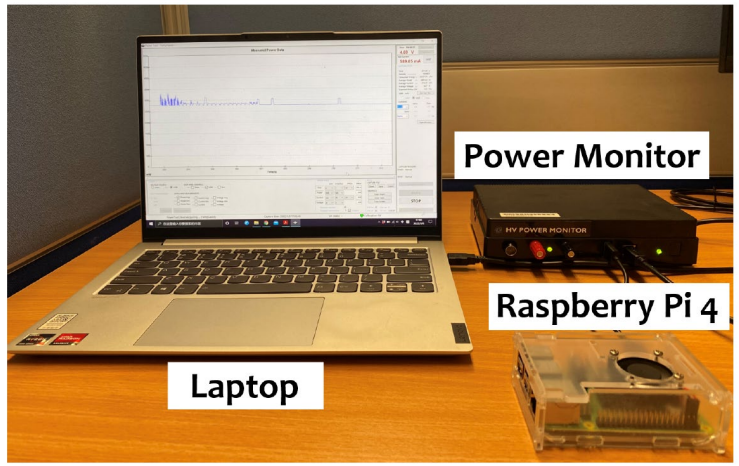
Test	Static Indoor	Mobile Outdoor	Static Indoor	Mobile Outdoor
Freq.	0.502	0.941	0.725	0.775
Block Freq.	0.321	0.743	0.709	0.757
Cumsum (Fwd).	0.621	0.821	0.609	0.802
Cumsum (Rev).	0.475	0.743	0.744	0.687
Runs.	0.917	0.089	0.492	0.121
Longest Run of 1's.	0.155	0.349	0.669	0.811
Approx. Entropy.	0.998	1.000	0.999	1.000
FFT.	0.281	0.293	0.541	0.729
Serial.	0.766	0.329	0.124	0.623

Key randomness

Experiment results

❑ Energy consumption

- ❖ Implement ChirpKey on a single board Raspberry Pi
- ❖ Use power monitor to evaluate the computation time and energy consumption



System implementation

TABLE III: Computation overhead.

User / Performance / Stage	Computation time (ms)		Energy consumption (mJ)	
	Alice	Bob	Alice	Bob
Channel variance estimation	1.98	0.22	7.843	-
Compression/reconstruction	0.0108	198	0.0713	-
Total	1.9908	198.22	7.9143	-

Energy consumption

Conclusion & future work

- We propose a fast and secure LoRa physical-layer key generation method—ChirpKey, which addresses two key limitations in existing work.

- ChirpKey can run real-time in current mobile devices and incur low system overhead.

- Future work will be focused on PCS-based secret key generation for large group LoRa nodes.

Thank you!