Trustworthy Autonomous Systems
RS-2C Securing the Communication Surface

Research Fellow: Dr. Zhuangkun Wei
Investigator: Prof. Weisi Guo
School of Aerospace, Transport and Manufacturing (SATM), Cranfield University, UK

Introduction

Communications of autonomous systems are vulnerable to attacks and eavesdropping, due to

- broadcasting communication nature
- the lack of randomness of the line-of-sight (LoS) dominated communication channels

Key-less PLS vs PL-SKG

Key-less physical layer security (key-less PLS):
maximize secrecy rate or signal-to-interference-noise-ratio (SINR), by optimizing trajectory, beamforming, IRS phase.
Advantage: key-less, easy deployment
Disadvantage: no solution guarantee when combined with mission & control layers objectives & constraints

Physical Layer Secret Key Generation (PL-SKG):
Generate shared secret sky via the reciprocal small-scale channel randomness.
Advantages: detached from mission & control layer optimization
Disadvantages: requires sufficient small-scale scattering & randomness

Contents

1. Secret Key Generation in IRS-aided LoS Channel

PL-SKG exploits the channel randomness & reciprocity between legitimate Alice and Bob. The vital step for PL-SKG is how to derive the reciprocal & random legitimate channel between Alice and Bob. Such channel probing results serve as the seed for further key generation.

How to derive common channel property

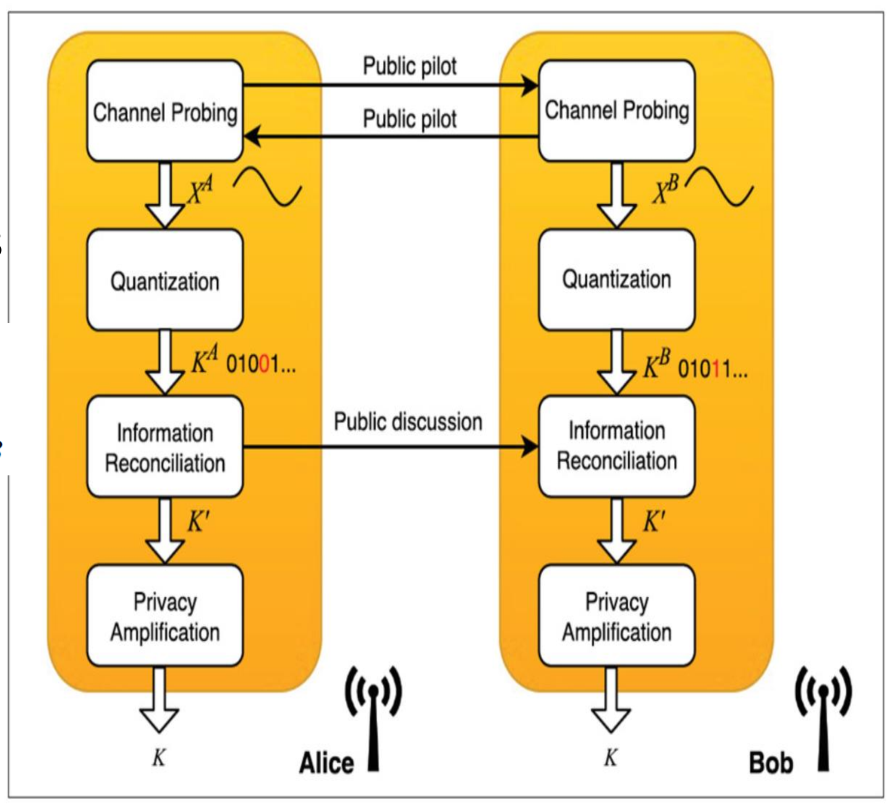
Step 1: IRS generate an independent IRS phase **w** for each channel estimation round.

Step 2: Alice and Bob send pilots $\mathbf{u}_A$ and $\mathbf{u}_B$ to each other in TDD mode. Alice's and Bob's received signals are:

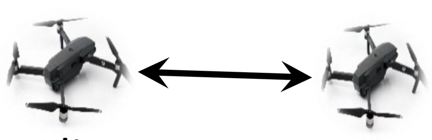
$$\mathbf{y}_A = (\mathbf{h}_{BA} + \mathbf{h}_{RA} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{BR}) \cdot \mathbf{u}_B + \boldsymbol{\epsilon}_A.$$
$$\mathbf{y}_B = (\mathbf{h}_{AB} + \mathbf{h}_{RB} \cdot diag(\mathbf{w})^H \cdot \mathbf{h}_{AR}) \cdot \mathbf{u}_A + \boldsymbol{\epsilon}_B$$

Step 3: Alice and Bob estimate the channel via the received signals, i.e.,

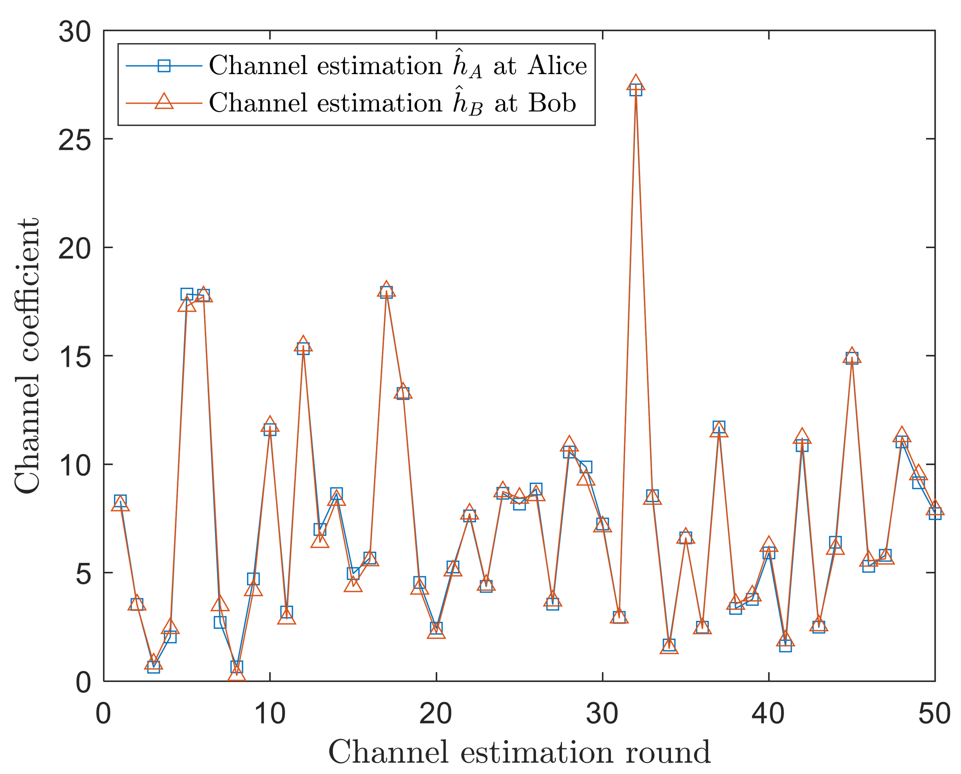
$$\hat{h}_A = \frac{\mathbf{u}_B^H \mathbf{y}_A}{\|\mathbf{u}_B\|_2^2} = (h_{BA} + \mathbf{h}_{RA} \cdot diag(\mathbf{w}) \cdot \mathbf{h}_{BR}) + \hat{\epsilon}_A$$
$$\hat{h}_B = \frac{\mathbf{u}_A^H \mathbf{y}_B}{\|\mathbf{u}_A\|_2^2} = (h_{AB} + \mathbf{h}_{RB} \cdot diag(\mathbf{w})^H \cdot \mathbf{h}_{AR}) + \hat{\epsilon}_B$$



Example



Secret Key	$\hat{h}_A$	h_{AB}	$\hat{h}_B$	Secret key
1	30.1	30	30.8	1
0	28.3	28	27.9	0
0	29.2	29	29.3	0
1	33.1	32	33.4	1
1	30.4	31	29.9	0
0	29.3	29	29.9	0

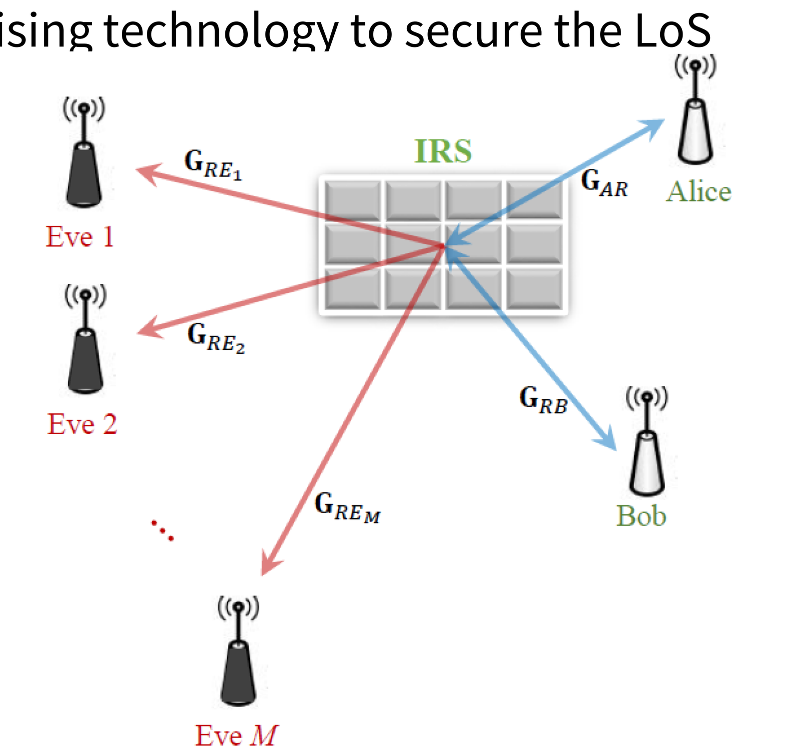


2. A Cooperative Eavesdropping Threat

Intelligent reflecting surface (IRS) is a promising technology to secure the LoS dominated low-entropy channels, by:

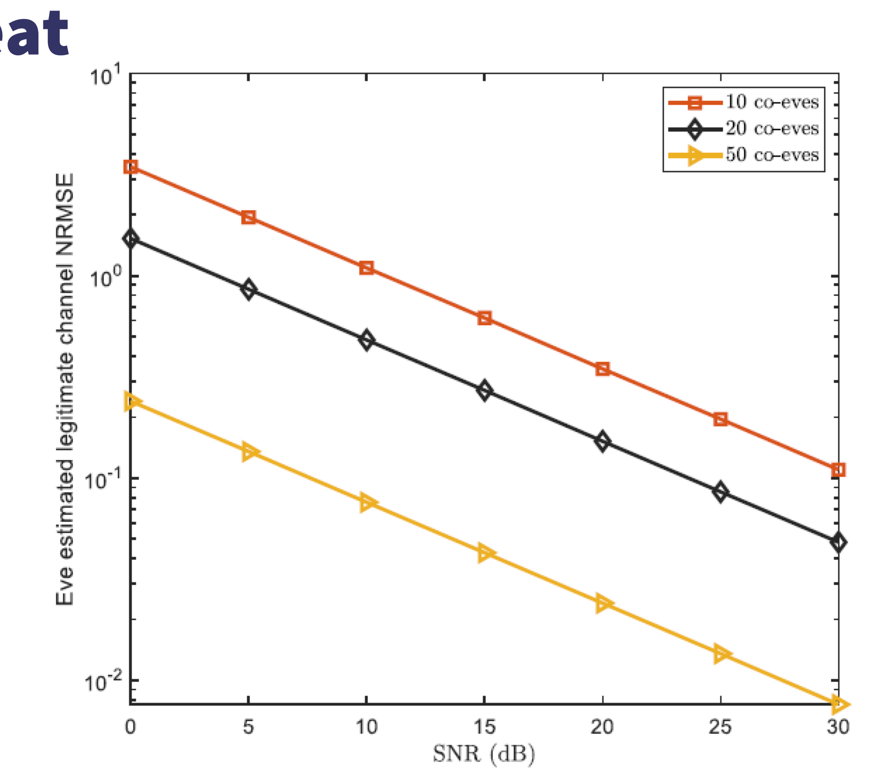
- Induce randomness via IRS phases
- Extra space for beamforming
- Artificial noise for anti-jamming

However, the IRS-induced randomness is also contained in the Eves' received signals, which enables the estimation of the legitimate channel by multiple & cooperative Eves.



Theory behind Multi-Eve Threat

The deployment of *N* Eves is to ensure the mutual information between *N* Eves' received signals and the legitimate channel equal the information entropy of the latter, which suggests a successful estimation of the legitimate channel from Eves.

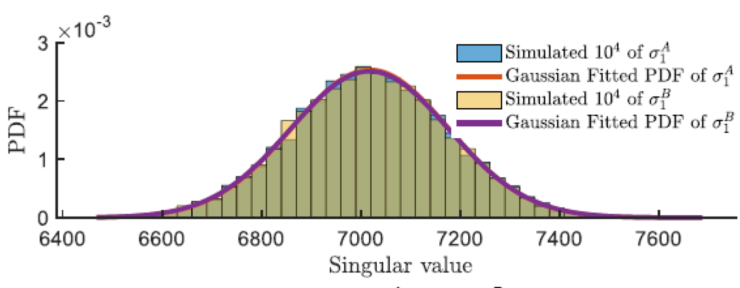


3. Random-Matrix based PL-SKG

Recalling from the Multi-Eve design that the prerequisite of channel estimation by Eves is the known of pilot sequences $\mathbf{u}_A$,$\mathbf{u}_B$. This inspires us to use random matrices instead of the public known pilot sequences. And this is random-matrix based PL-SKG.

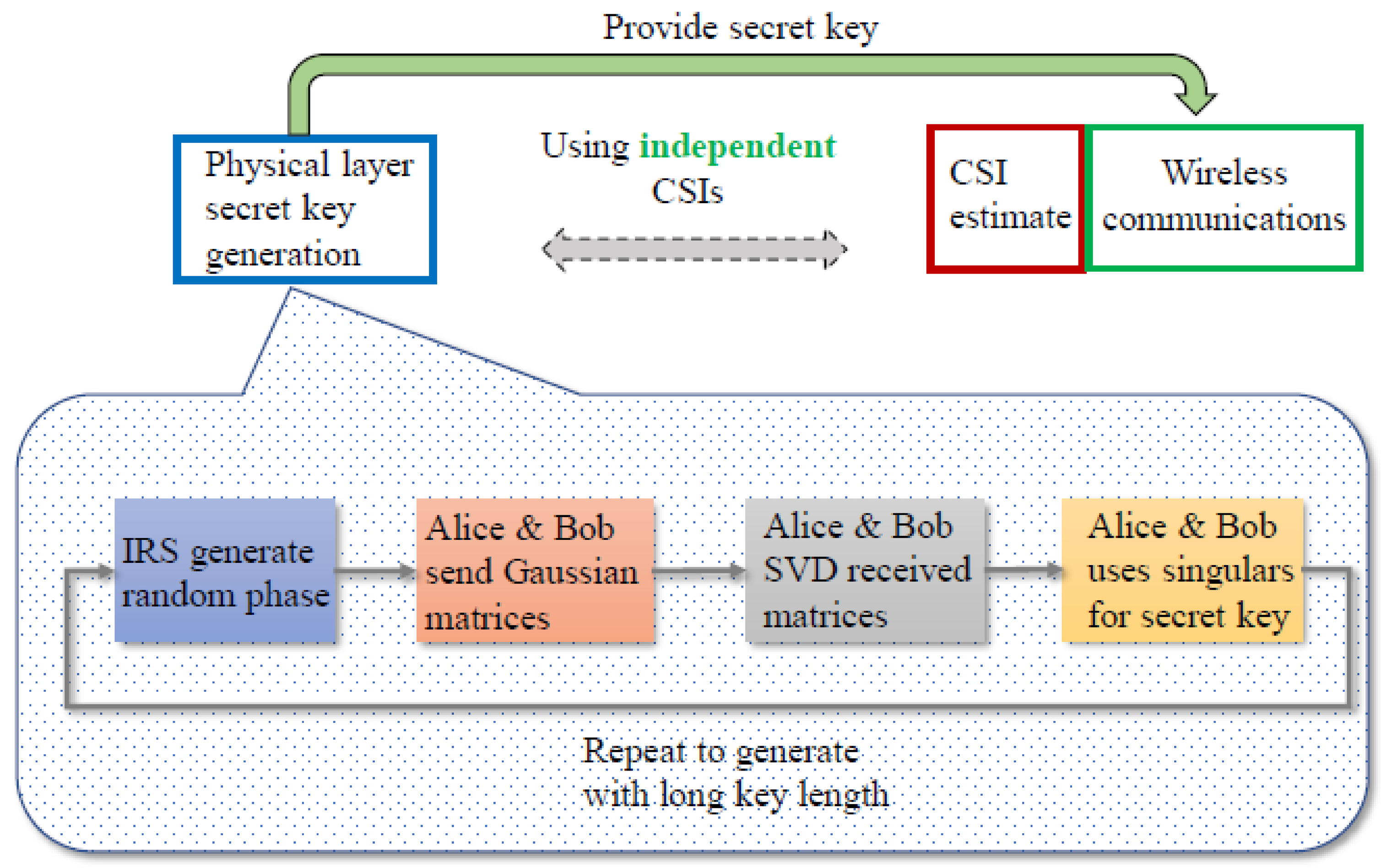
Theory of Random-Matrix based PL-SKG

Theorem 1: Consider a matrix $\mathbf{H} \in \mathbb{C}^{N\times L}$, and two random matrices $\mathbf{X}_1 \in \mathbb{C}^{N\times D}$ and $\mathbf{X}_2 \in \mathbb{C}^{L\times D}$, where elements are i.i.d and follow the normal complex Gaussian distribution, i.e., $\mathcal{CN}(0,1)$. Then, the singular values of $\mathbf{H}\cdot\mathbf{X}_1$ and of $\mathbf{H}^H\cdot\mathbf{X}_2$, denoted as $\boldsymbol{\sigma}(\mathbf{H}\mathbf{X}_1)$ and $\boldsymbol{\sigma}(\mathbf{H}^H\mathbf{X}_2)$, follow the same probability distribution.

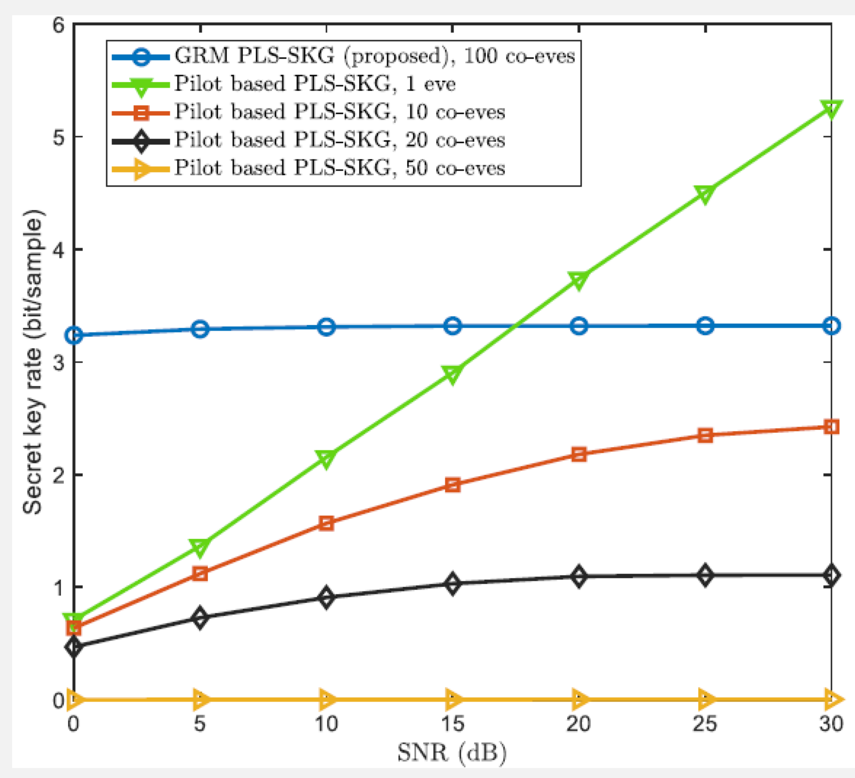


(a) Identical PDFs of σ_i^A and of σ_i^B, under fixed IRS w

Sketch of Random-Matrix based PL-SKG



Results



The result shows our proposed random matrix based PL-SKG:

(i) comparatively superior (up to 300%) secret key rate in low SNR regime, attributed to the noise resistance ability of the singular values

(ii) generally improved secret key rate performance against Multi-Eves.

This work is supported, in part, by the Engineering and Physical Sciences Research Council [grant number: EP/V026763/1]