# Article information:

CSI-Based Versus RSS-Based Secret-Key Generation Under Correlated Eavesdropping | IEEE Journals & Magazine | IEEE Xplore
<https://ieeexplore.ieee.org/abstract/document/9270035>

# Article summary:

1. This article investigates and compares the secret-key capacity based on the sampling of the entire complex channel state information (CSI) or only its envelope, the received signal strength (RSS).

2. It takes into account that the eavesdropper's observations might be correlated and considers the high signal-to-noise ratio (SNR) regime.

3. At high SNR, it is able to precisely quantify a penalty for RSS-based secret-key generation: a halved pre-log factor and a constant penalty of about 0.69 bit, which disappears as Eve's channel gets highly correlated.

# Article rating:

Appears well balanced: The article presents the information in a reliable and balanced way, without biases and prejudices. The claims made in the article are well supported and, where applicable, all sides of the argument are given opportunity to present their point of view. The article appears trustworthy and reliable.

# Article analysis:

This article provides an in-depth analysis of two methods for generating secret keys between two legitimate users (Alice and Bob), subject to an illegitimate user (Eve) trying to recover the key. The article is well written and provides clear explanations of both methods, as well as their respective advantages and disadvantages. The authors provide detailed analysis of both methods in terms of their secret key capacity, taking into account that the eavesdropper's observations might be correlated and considering the high signal-to-noise ratio (SNR) regime. The authors also provide precise quantitative results for both methods at high SNR, which can be used to compare them more accurately.

The article does not appear to have any major biases or one-sided reporting; it presents both methods fairly and objectively without promoting either one over the other. All claims are supported by evidence from previous works in this field, making them reliable and trustworthy. There are no missing points of consideration or unexplored counterarguments; all relevant information is presented in detail. Furthermore, possible risks associated with each method are noted throughout the article, providing readers with a comprehensive understanding of each method’s strengths and weaknesses. In conclusion, this article is reliable and trustworthy due to its thorough analysis of both methods for generating secret keys under correlated eavesdropping conditions.

# Topics for further research:

* Secret key capacity
* Correlated eavesdropping
* High signal-to-noise ratio
* Key generation methods
* Security risks
* Quantitative results

# Report location:

<https://www.fullpicture.app/item/33bff888b089d16a30edd62b29c683f6>