Physical Layer Security on Software Defined Radio

KEVIN RYLAND

VIRGINIA TECH

09/14/17

OVERVIEW

- Intro to Physical Layer Security
- Background Information
- Artificial Noise Generation
- Implementation
- Ongoing and Future Work

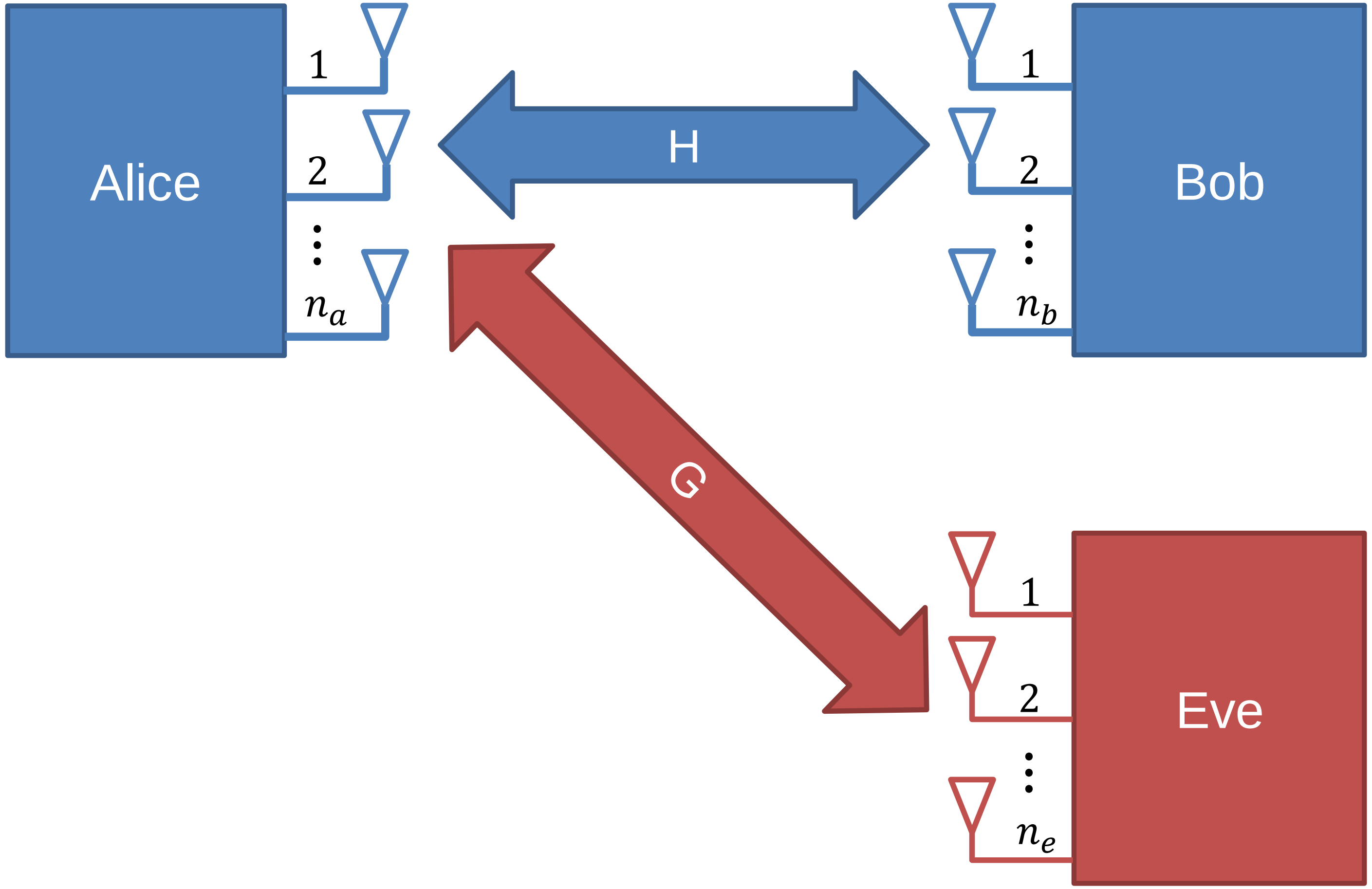
OVERVIEW

- Intro to Physical Layer Security
- Background Information
- Artificial Noise Generation
- Implementation
- Ongoing and Future Work

PHYSICAL LAYER SECURITY

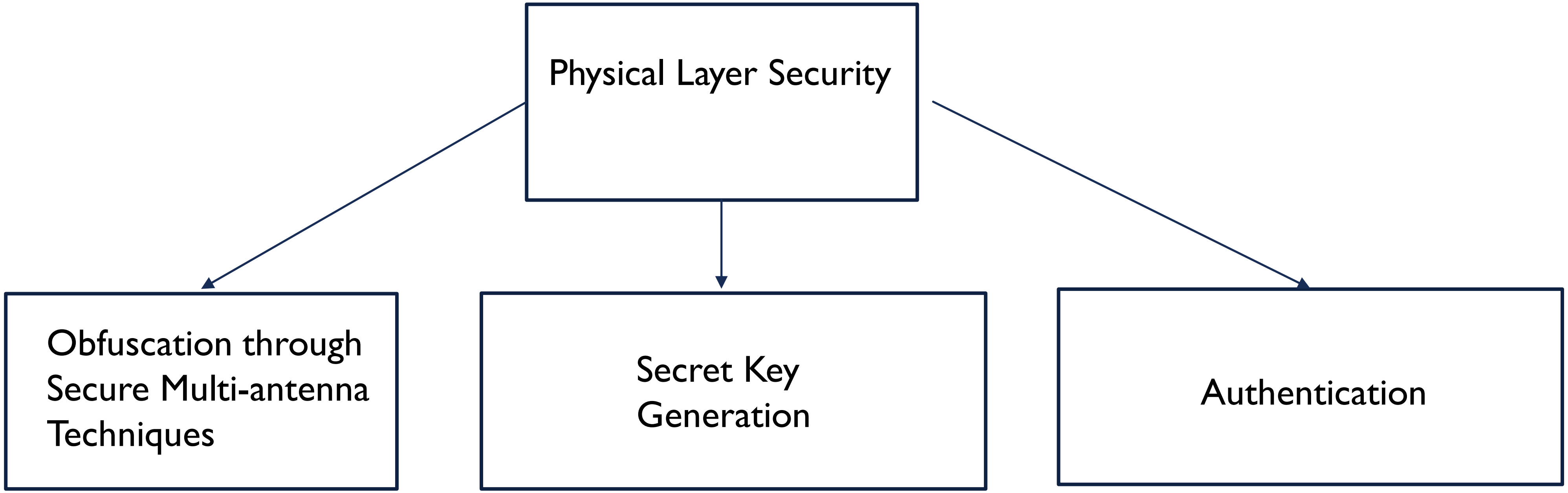
- Dates back to the 1970s with a mathematical description of a wiretap channel
- Advancements in MIMO and integration into technologies such as 802.11n and LTE have created a resurgence of PLS research in the last decade geared towards exploiting MIMO for security benefits
- A major focus of PLS techniques is to exploit the unique characteristics of the channel between the intended communicants to provide the intended receiver with an advantage over eavesdroppers

NAMING CONVENTION



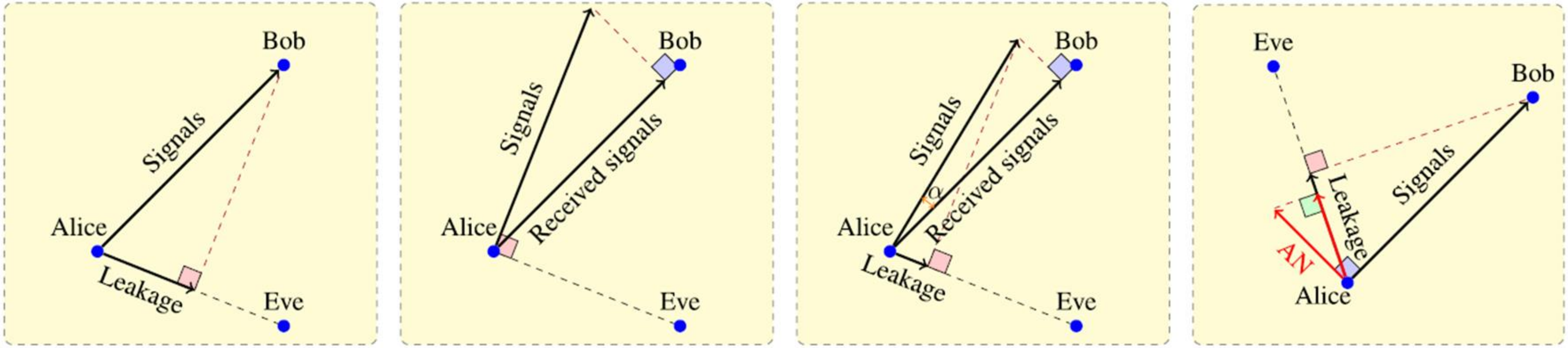
Source: https://xkcd.com/1323/

Principal Areas



SECURE MULTI-ANTENNA TECHNIQUES

Source: Yi-Sheng Shui, *Physical Layer Security in Wireless Networks: A Tutorial*

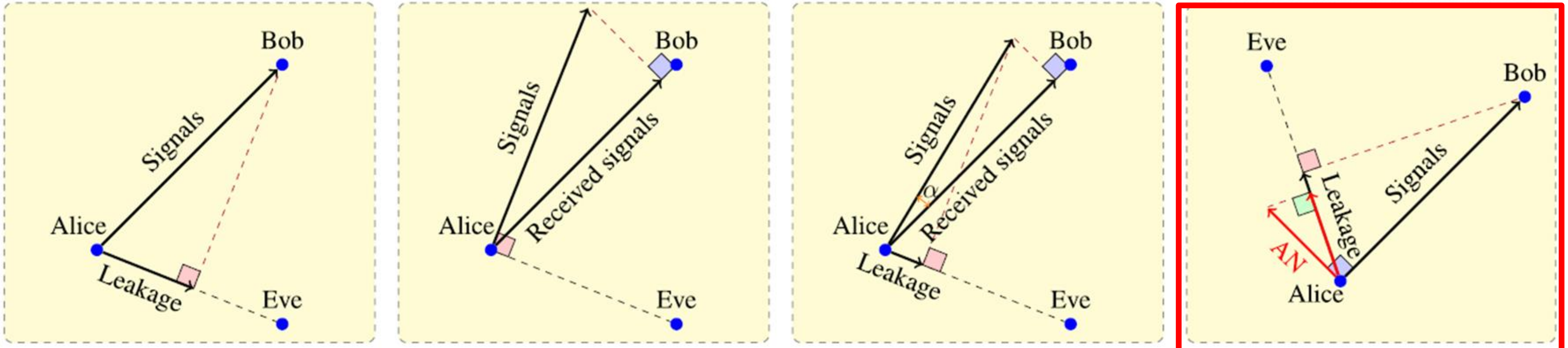


(a) Beamforming. (b) ZF precoding. (c) CVX-based precoding. (d) AN precoding.

- **Beamforming** – use Bob's CSI to provide a maximized gain with no regard for leakage into Eve's channel.
- **ZF Precoding** – use Eve's CSI to transmit message orthogonal to Eve, this is equivalent to steering a null at Eve.
- **CVX Precoding** – use convex optimization software to optimize between beamforming to Bob and steering a null at Eve. This is the only secrecy capacity-achieving scheme, but is computationally expensive.
- **AN Precoding** – beamforming to Bob while transmitting noise in Bob's nullspace. Does not require Eve's CSI.

SECURE MULTI-ANTENNA TECHNIQUES

Source: Yi-Sheng Shui, *Physical Layer Security in Wireless Networks: A Tutorial*



(a) Beamforming. (b) ZF precoding. (c) CVX-based precoding. (d) AN precoding.

My Research Focus

- **Beamforming** – use Bob's CSI to provide a maximized gain with no regard for leakage into Eve's channel.
- **ZF Precoding** – use Eve's CSI to transmit message orthogonal to Eve, this is equivalent to steering a null at Eve.
- **CVX Precoding** – use convex optimization software to optimize between beamforming to Bob and steering a null at Eve. This is the only secrecy capacity-achieving scheme, but is computationally expensive.
- **AN Precoding** – beamforming to Bob while transmitting noise in Bob's nullspace. Does not require Eve's CSI.

PHYSICAL LAYER KEY GENERATION

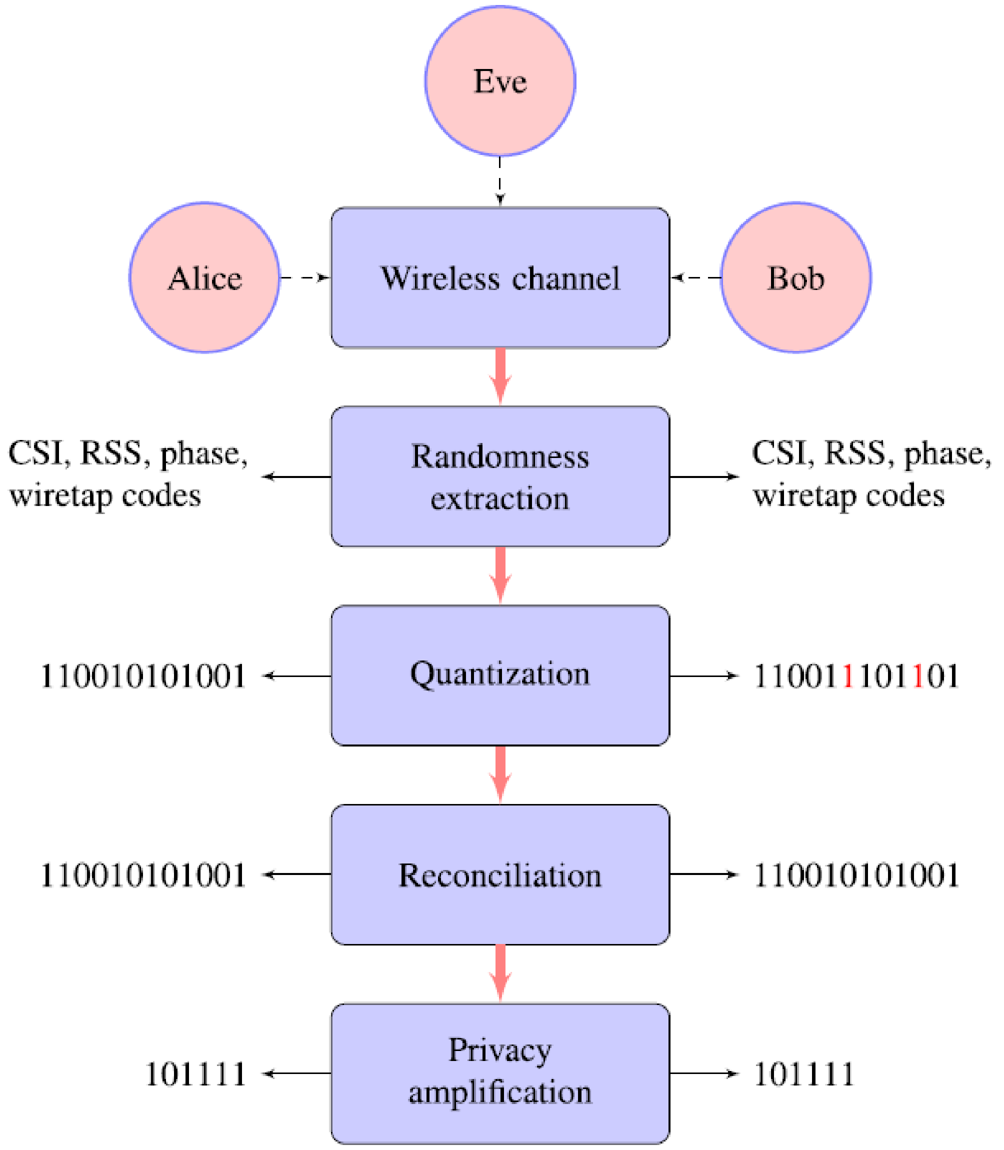
- Requires Alice and Bob to measure a shared characteristic unique to their connection in the presence of an eavesdropper
- Examples of the characteristics are: full CSI, RSSI, channel phase, and wiretap codes
- The tricky part with implementing PLS key gen is balancing the uniqueness of the measurement with how easy it is for Alice and Bob to independently measure it

For example:

Alice measures RSSI to be 5.439 and Bob measures it to be 5.428

Eve's close to Bob and measures RSSI to be 4.932

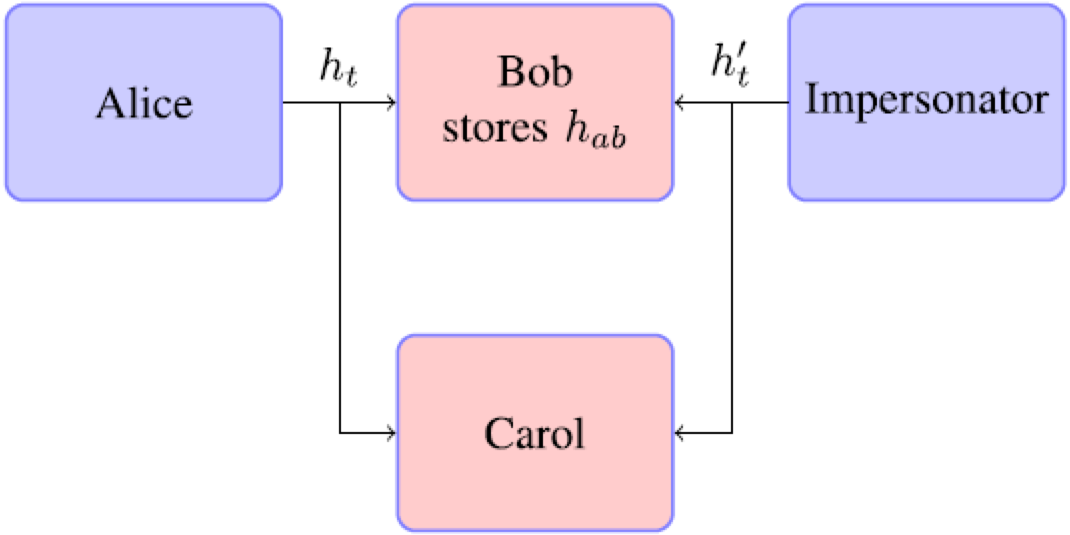
To insure coordination between Alice and Bob, we should round the measurement to 5.4. Eve can round to 5.0, so to avoid Eve having knowledge of the key, we also remove the most significant figure which results in Alice and Bob measuring .4 while Eve measures .0



Source: Yi-Sheng Shui, *Physical Layer Security in Wireless Networks: A Tutorial*

PHYSICAL LAYER AUTHENTICATION

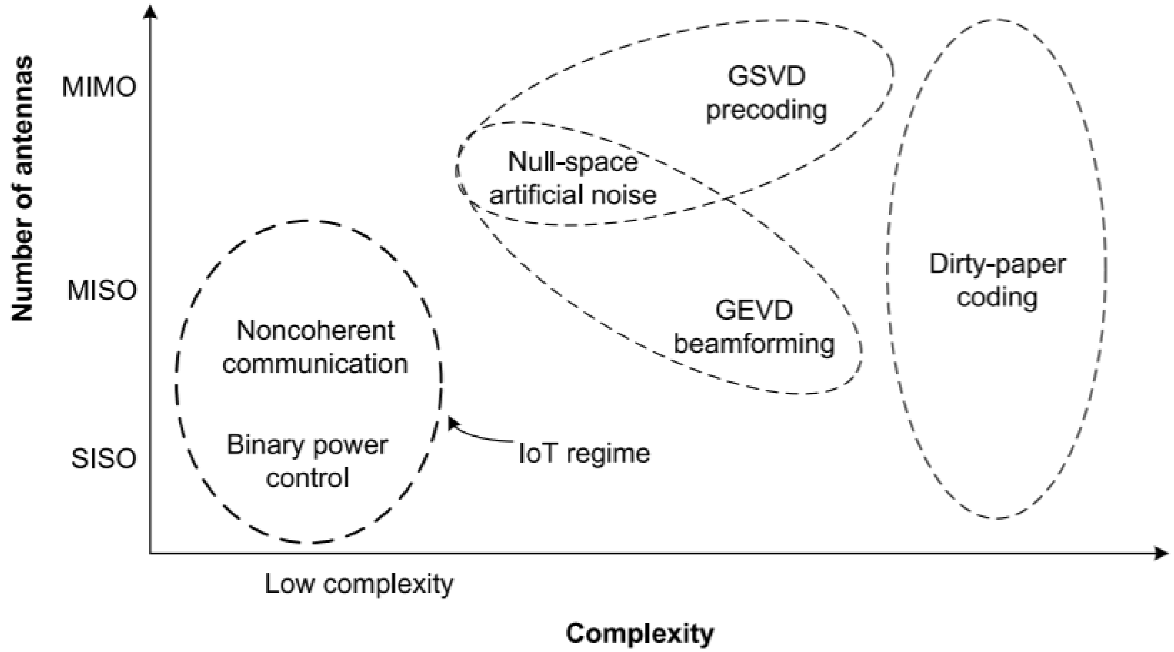
- Bob needs to initially store Alice's channel, which can then be used to verify subsequent transmissions
- Verification is done through a combination of channel estimation and hypothesis testing
- Relies on independent channel fading for Alice and the Impersonator
- Bob and Carol can both receive Alice and the Impersonator's signals, but only Bob will be able to authenticate



Source: Yi-Sheng Shui, *Physical Layer Security in Wireless Networks: A Tutorial*

APPLIED RESEARCH FOR PHYSICAL LAYER SECURITY

- Large M2M networks where key/certificate management is burdensome – Internet of Things
- Easy integration with existing cryptographic security
- PHYLAWS – EU Consortium focusing on practically evaluating physical layer security techniques and exploring implementations for new wireless standards



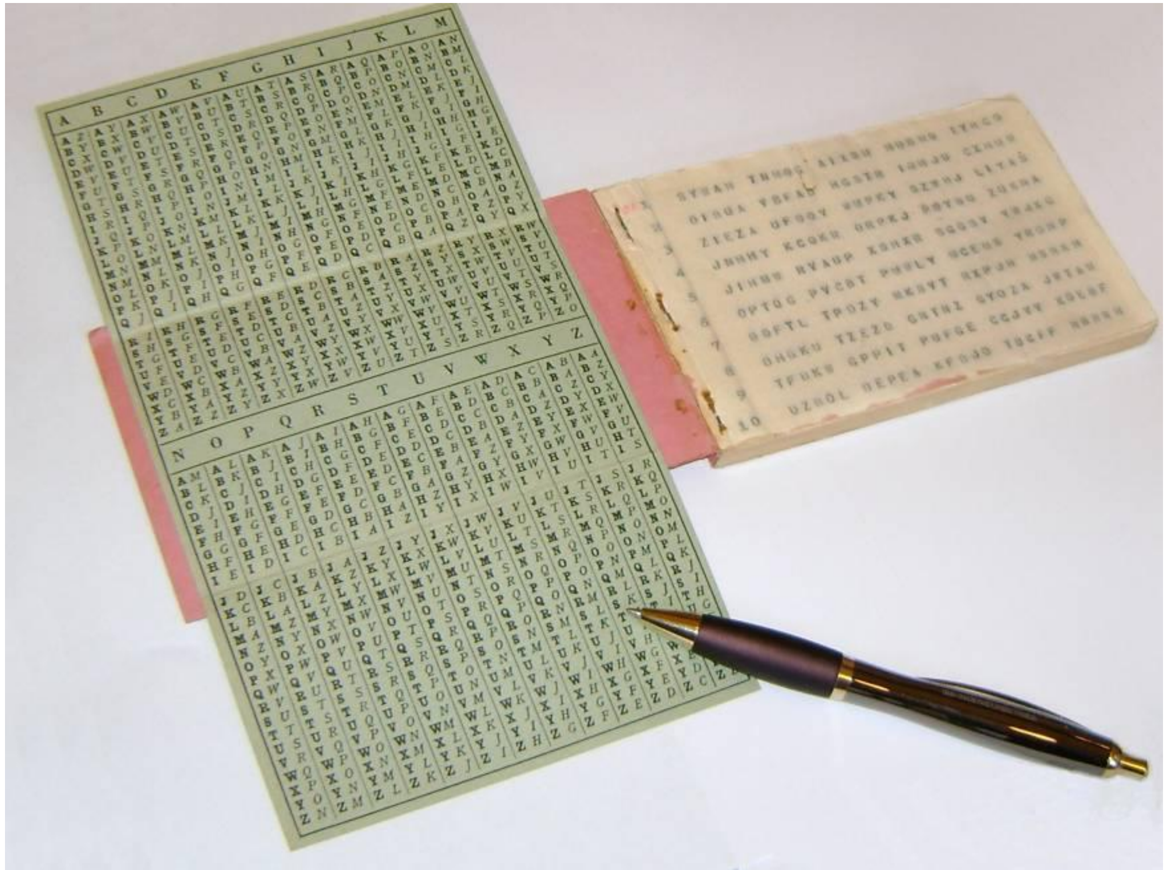
Source: Amativ Mukherjee, *Physical Layer Security in the Internet of Things*

SEVENTH FRAMEWORK PROGRAMME

OVERVIEW

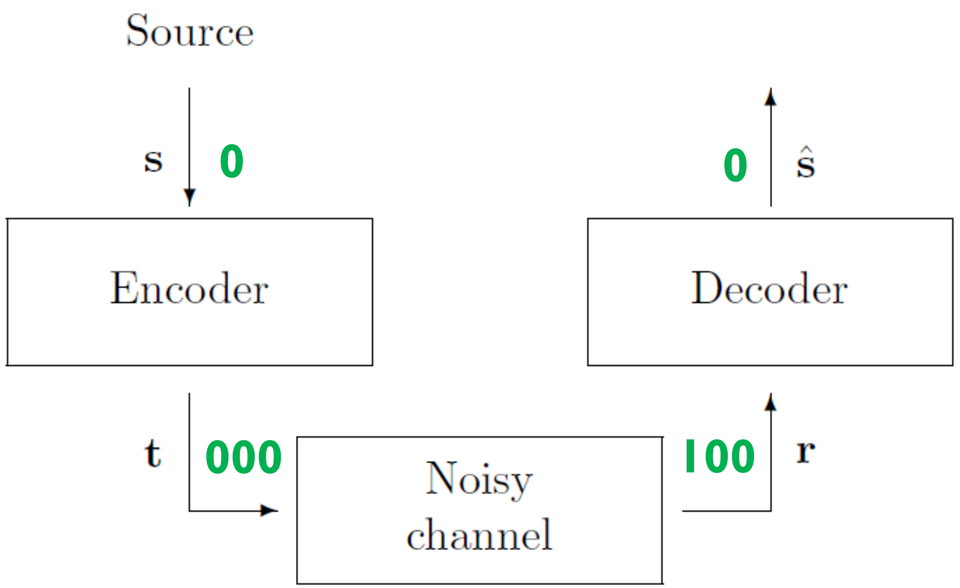
- Intro to Physical Layer Security
- Background Information
- Artificial Noise Generation
- Implementation
- Ongoing and Future Work

INFORMATION THEORETIC SECURITY



ERROR CORRECTION CODING

- Error correction codes add redundancy to correct for errors that the transmitted data experiences in a channel



Example: Repetition Coding

Source (s)	Transmitted (t)
0	000
1	111

Recevied (r)	Decoded (ŝ)
000	0
001	0
010	0
011	1
100	0
101	1
110	1
111	1

SHANNON CHANNEL CAPACITY

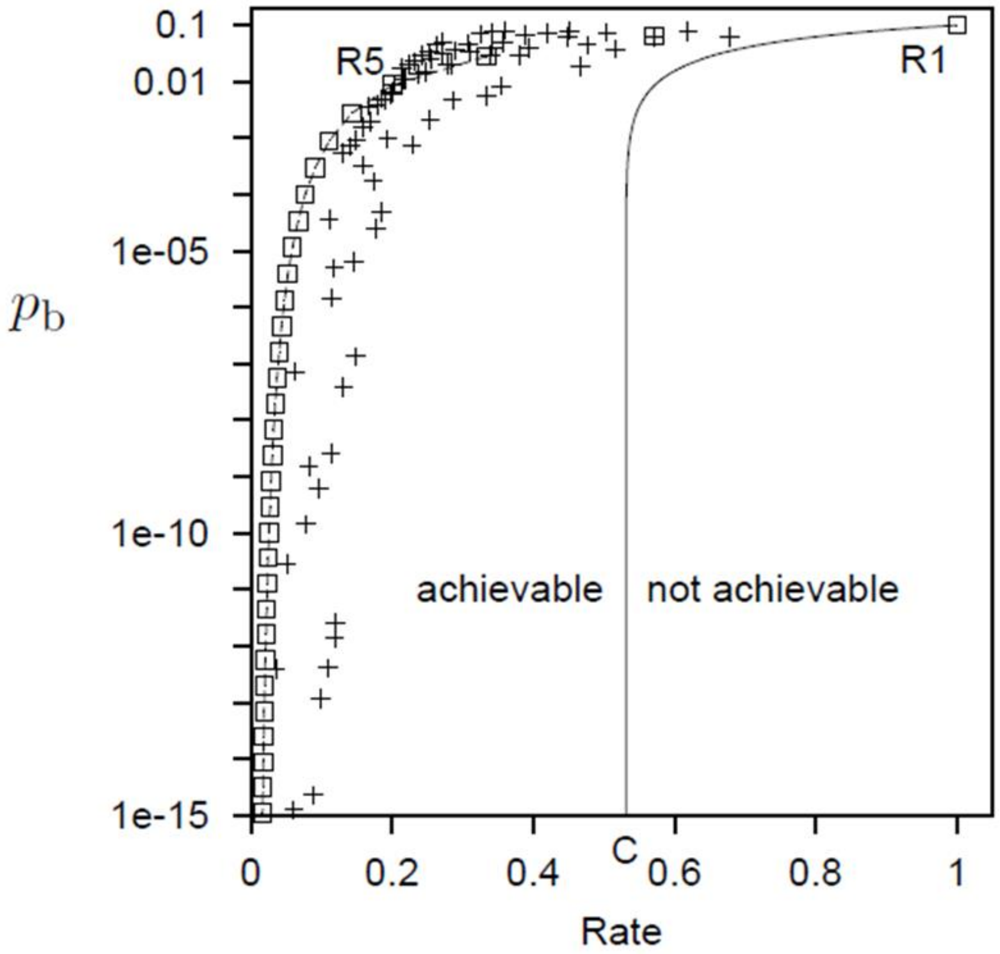
- Each code has a rate defined by the ratio of transmitted bits to the total code length

$$Rate = \frac{\#\,TX\ Bits}{Code\ Length}$$

- Shannon defined the **channel capacity**, C, as the smallest code rate that achieves an arbitrarily small BER
- The capacity of a AWGN channel is

$$C = Blog_2(1 + SNR)$$

BSC with flip probability, f = 0.1



Source: David Mackay, Information Theory, Inference, and Learning Algorithms

HOW CAN WE MEASURE INFORMATION?

- “Did you know the sun’s going to rise tomorrow?”
  - 47 Characters
  - Very little information
- “There’s going to be a huge storm tonight.”
  - 40 Characters
  - A lot of information

HOW CAN WE MEASURE INFORMATION?

- The **Shannon Information Content** of an outcome, x, is defined as:

$$h(x) = \log_2 \frac{1}{P(x)}$$

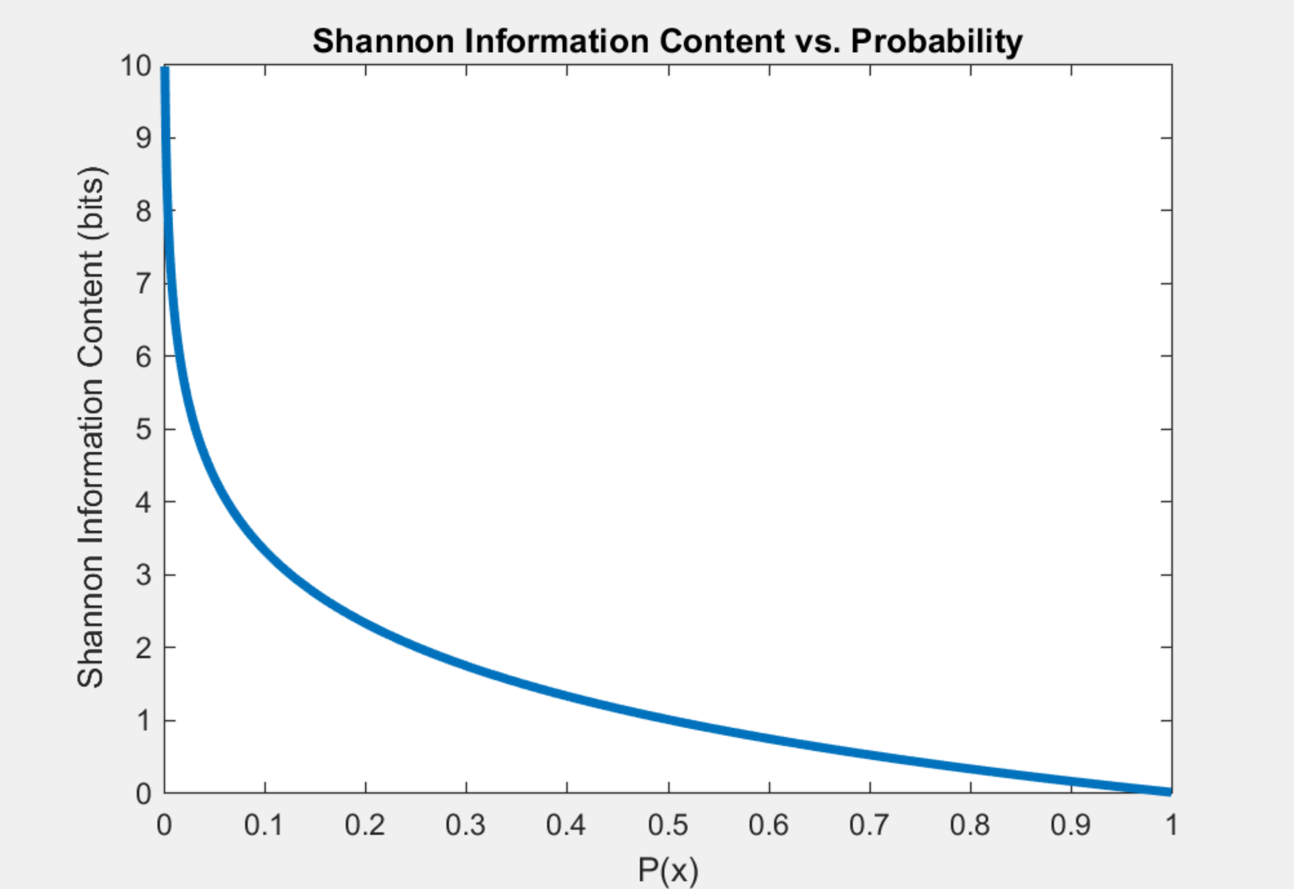
- Rare outcomes contain more information than common outcomes

"The Sun is going to Rise Tomorrow Morning."

$$P \approx 1 \Rightarrow h \approx 0$$

"GNU Radio installed with no problems."

$$P \approx 0 \Rightarrow h \approx \infty$$



HOW CAN WE MEASURE INFORMATION?

- An Ensemble, $X = (x, A_X, P_X)$, is defined as a set of outcomes, x, that take on a set of values, A_X, with corresponding probabilities, P_X.
- The **Entropy** of an ensemble, X, is defined as the average of the Shannon Information Content over its set of outcomes:

$$H(X) = \sum_{x \in A_X} P(x) \log_2 \left(\frac{1}{P(x)} \right) = \sum_{x \in A_X} P(x) h(x)$$

- The Entropy of a randomly selected English letter is:

$$H(X) = 4.11 \text{ bits}$$

i	a_i	p_i	$h(p_i)$
1	a	.0575	4.1
2	b	.0128	6.3
3	c	.0263	5.2
4	d	.0285	5.1
5	e	.0913	3.5
6	f	.0173	5.9
7	g	.0133	6.2
8	h	.0313	5.0
9	i	.0599	4.1
10	j	.0006	10.7
11	k	.0084	6.9
12	l	.0335	4.9
13	m	.0235	5.4
14	n	.0596	4.1
15	o	.0689	3.9
16	p	.0192	5.7
17	q	.0008	10.3
18	r	.0508	4.3
19	s	.0567	4.1
20	t	.0706	3.8
21	u	.0334	4.9
22	v	.0069	7.2
23	w	.0119	6.4
24	x	.0073	7.1
25	y	.0164	5.9
26	z	.0007	10.4
27	-	.1928	2.4

Source: David Mackay, Information Theory, Inference, and Learning Algorithms

MUTUAL INFORMATION/CHANNEL CAPACITY

- Mutual Information, $I(X;Y)$, is a measure of the amount of information X conveys about Y

$$I(X;Y) = H(X) - H(X|Y)$$

- Channel Capacity, C, is the maximum Mutual Information achievable by optimizing the input distribution, P_x

$$C = \max_{P_x} I\ (X;Y)$$

WYNER WIRETAP CHANNEL

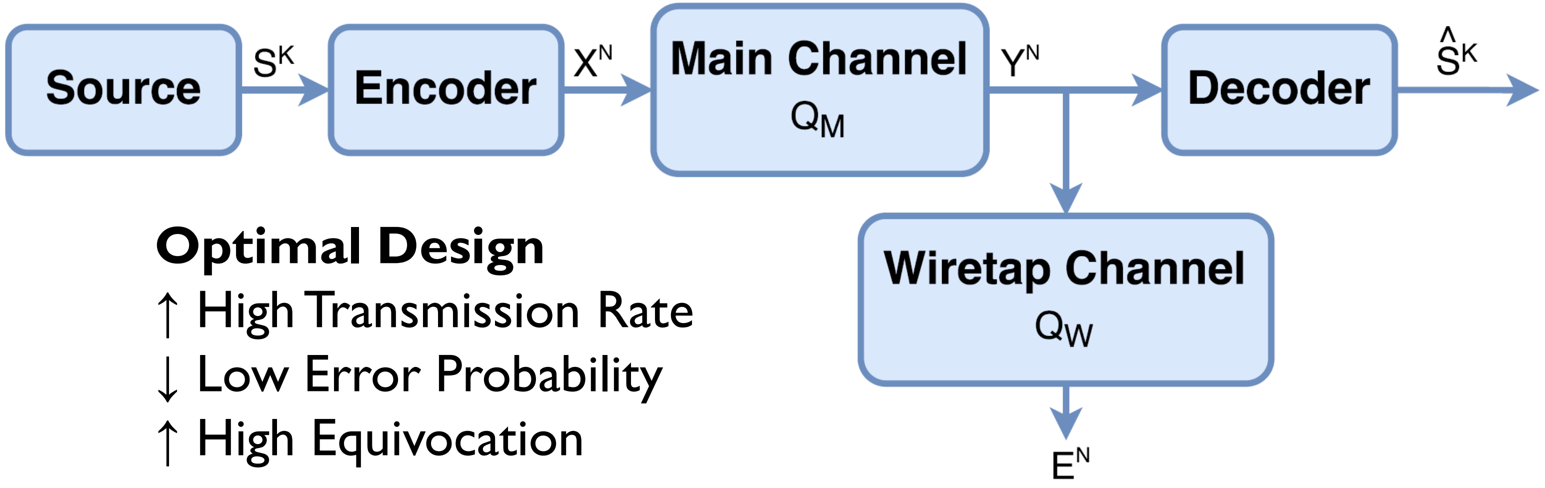
- **Transmission Rate (bits/channel use)**

Proportion of information sent in each code word

$$R \;= H_S K/N$$

- **Equivocation Rate** – measure of confusion at the eavesdropper

$$\Delta = \frac{1}{K} H(S^K|Z^N)$$



Optimal Design

↑ High Transmission Rate

↓ Low Error Probability

↑ High Equivocation

WYNER WIRETAP CHANNEL

Bob's Mutual Information: $I(S;Y) = H(S) - H(S|Y)$

Eve's Mutual Information: $I(S;Z) = H(S) - H(S|Z)$

Maximize the Difference: $\mathrm{C_S} = \max_{P_S}\big(I(S;Y) - I(S;Z)\big)$

WYNER WIRETAP CHANNEL

Bob's Mutual Information: $I(S;Y) = H(S) - H(S|Y)$

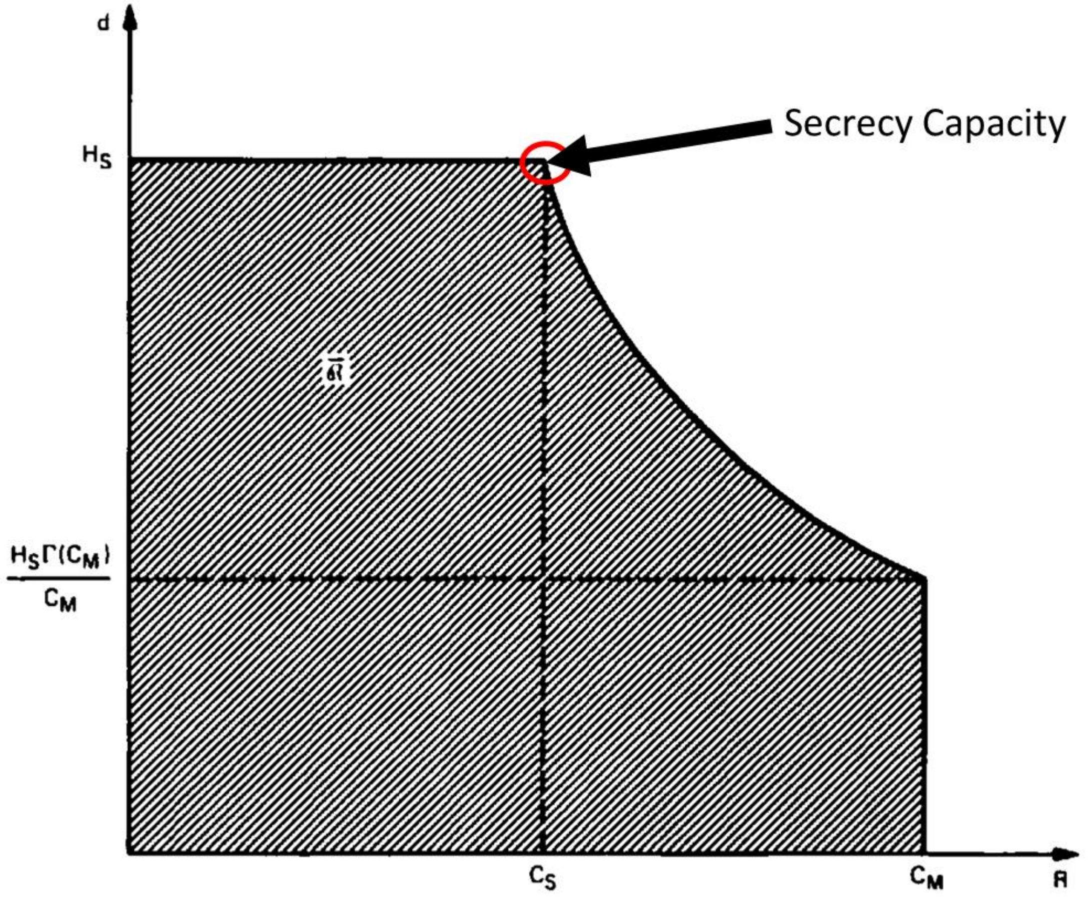
Eve's Mutual Information: $I(S;Z) = H(S) - \boxed{H(S|Z)}$ Equivocation Term!

Maximize the Difference: $C_S = \max_{P_S}\big(I(S;Y) - I(S;Z)\big)$

WYNER WIRETAP CHANNEL

- Wyner characterizes a region of achievable (R,d) pairs
  - R is the Transmission Rate
  - d is the Equivocation Rate
- The highest rate that achieves complete equivocation at the eavesdropper is the **secrecy capacity** of the channel
- The secrecy capacity for the wiretap channel is the difference in the capacity of Bob and Eve's channels

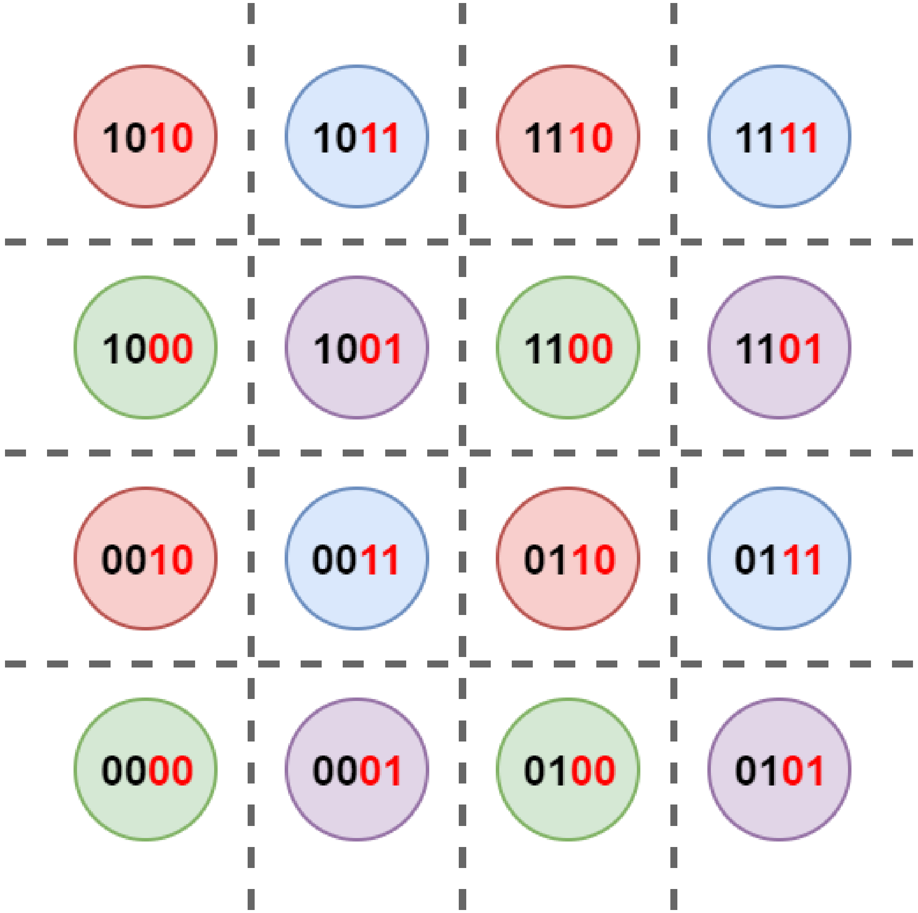
$$C_s = C_{Bob} - C_{Eve}$$



Source: A. D. Wyner, *The Wiretap Channel*

WYNER WIRETAP CODING EXAMPLE

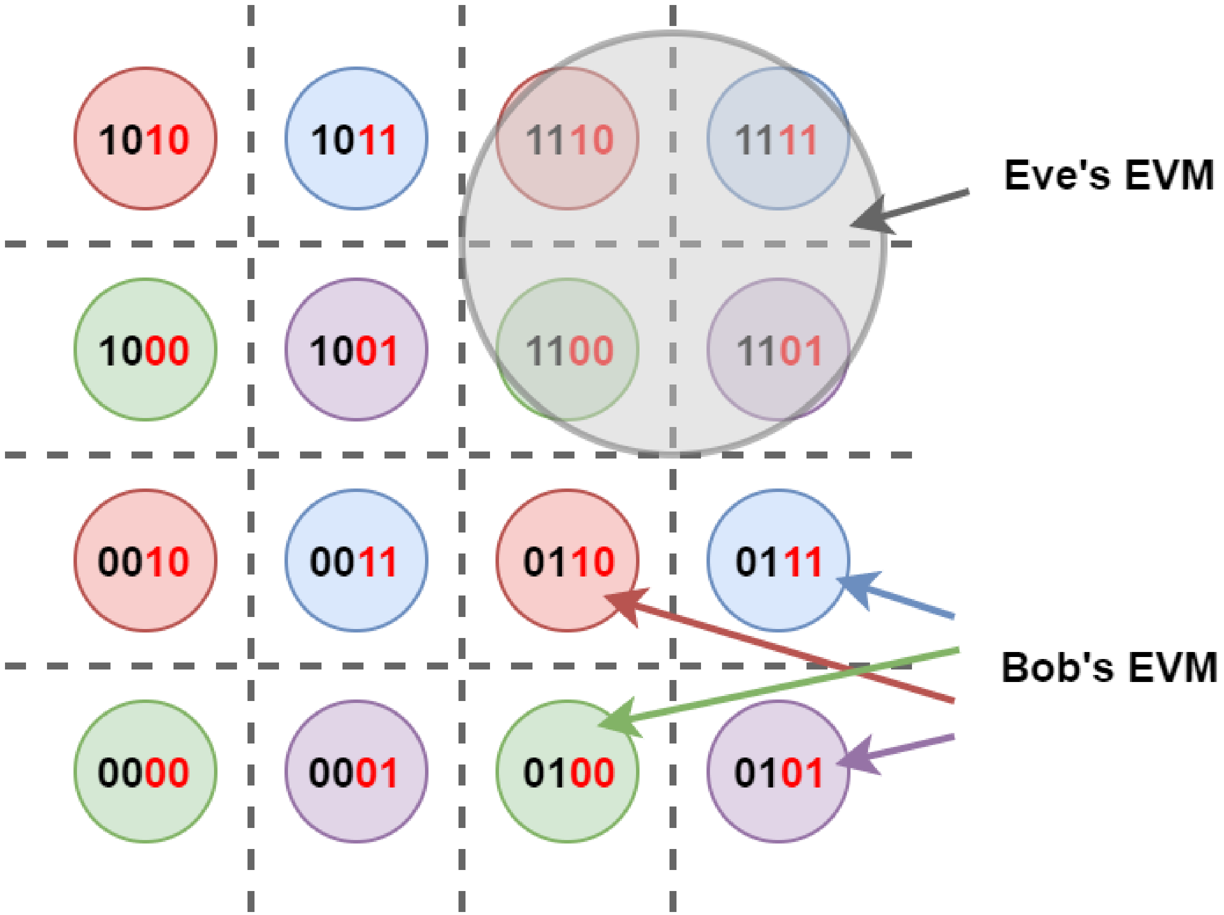
- **Unprotected Bits**
- **Protected Bits**



WYNER WIRETAP CODING EXAMPLE

- Bob's SNR is large enough to demodulate 16-QAM – EVM is at least smaller than a quarter of a quadrant

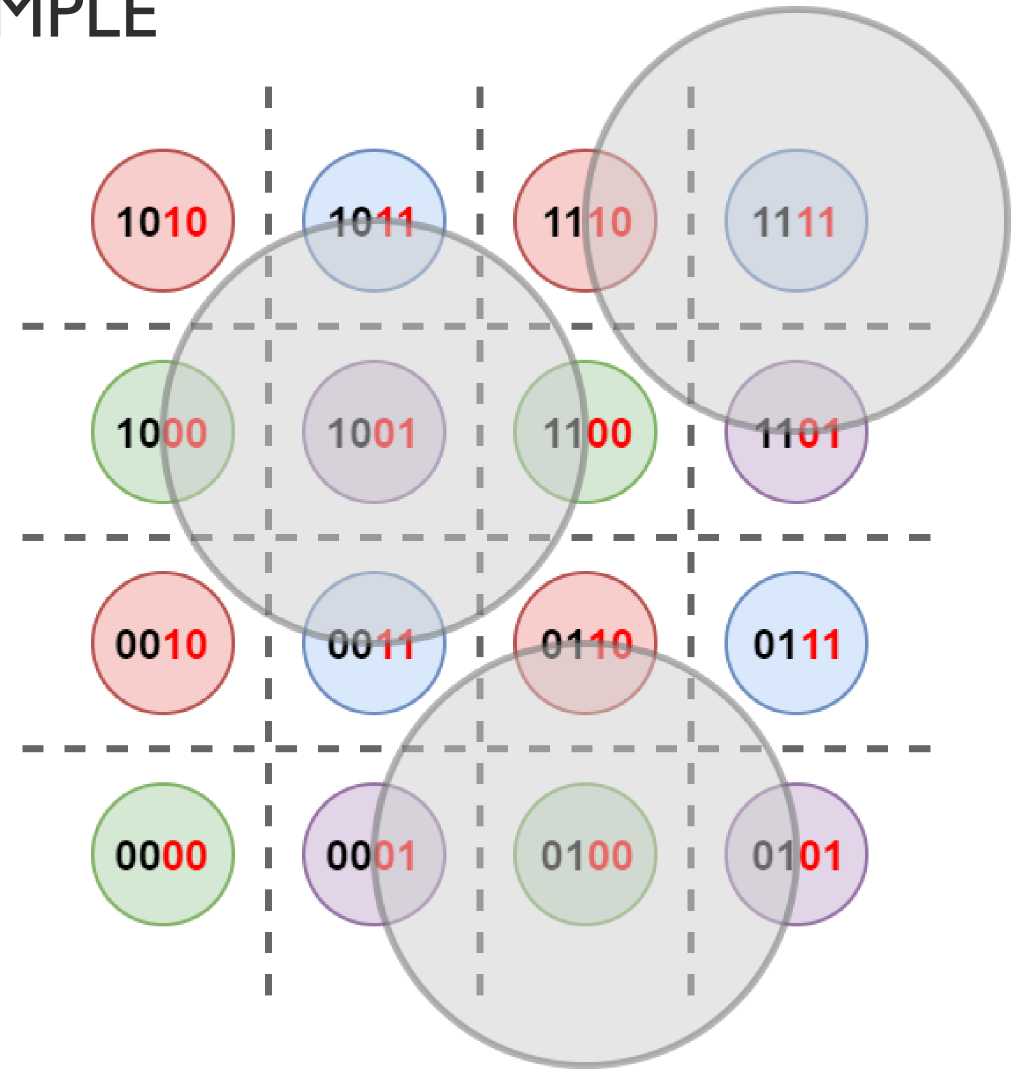
- Eve's SNR is only large enough to demodulate QPSK – EVM is the size of a quadrant



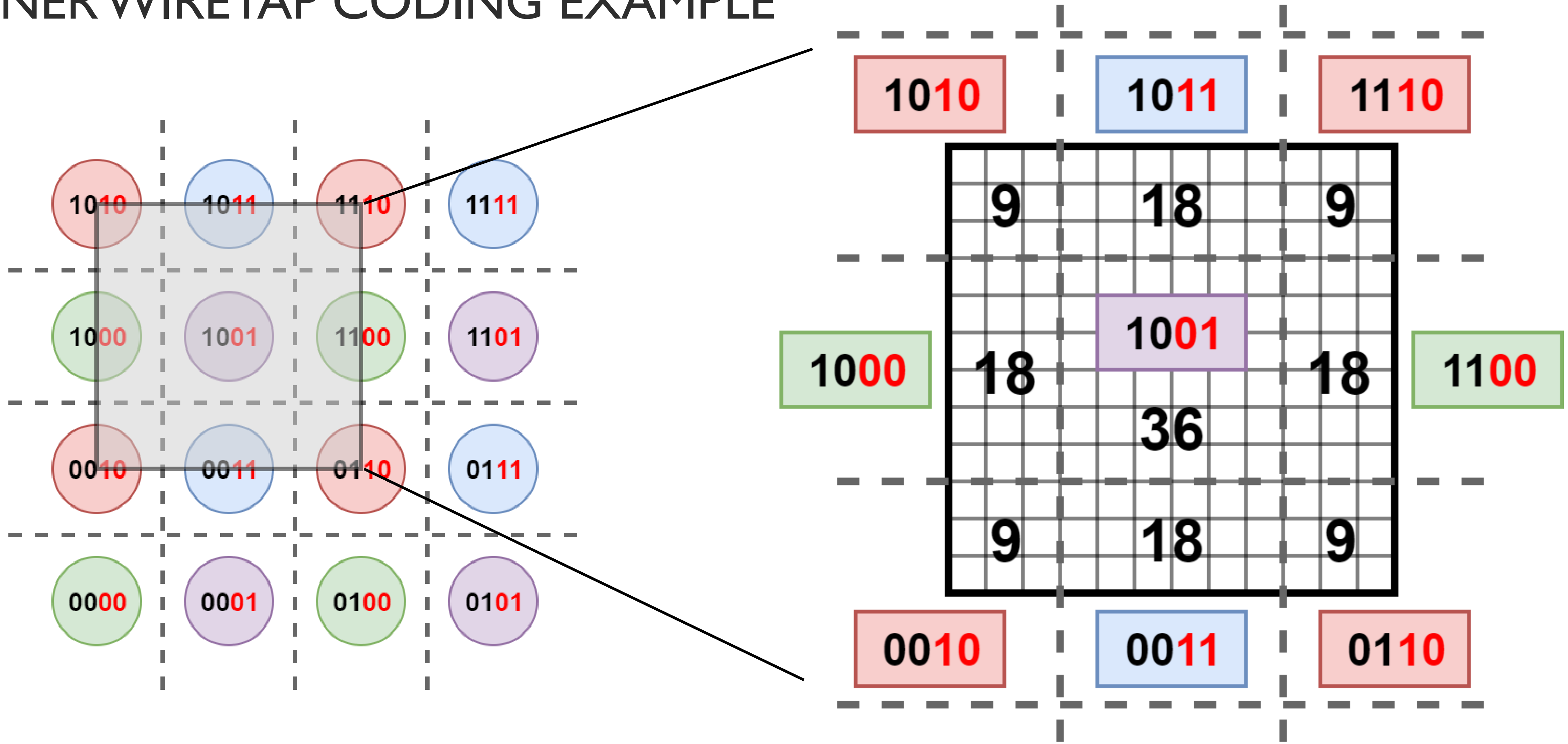
WYNER WIRETAP CODING EXAMPLE

- Eve makes ambiguous* decisions on protected bits

- Secrecy comes from a gap in instantaneous SNR, but we control what gets protected through coding!



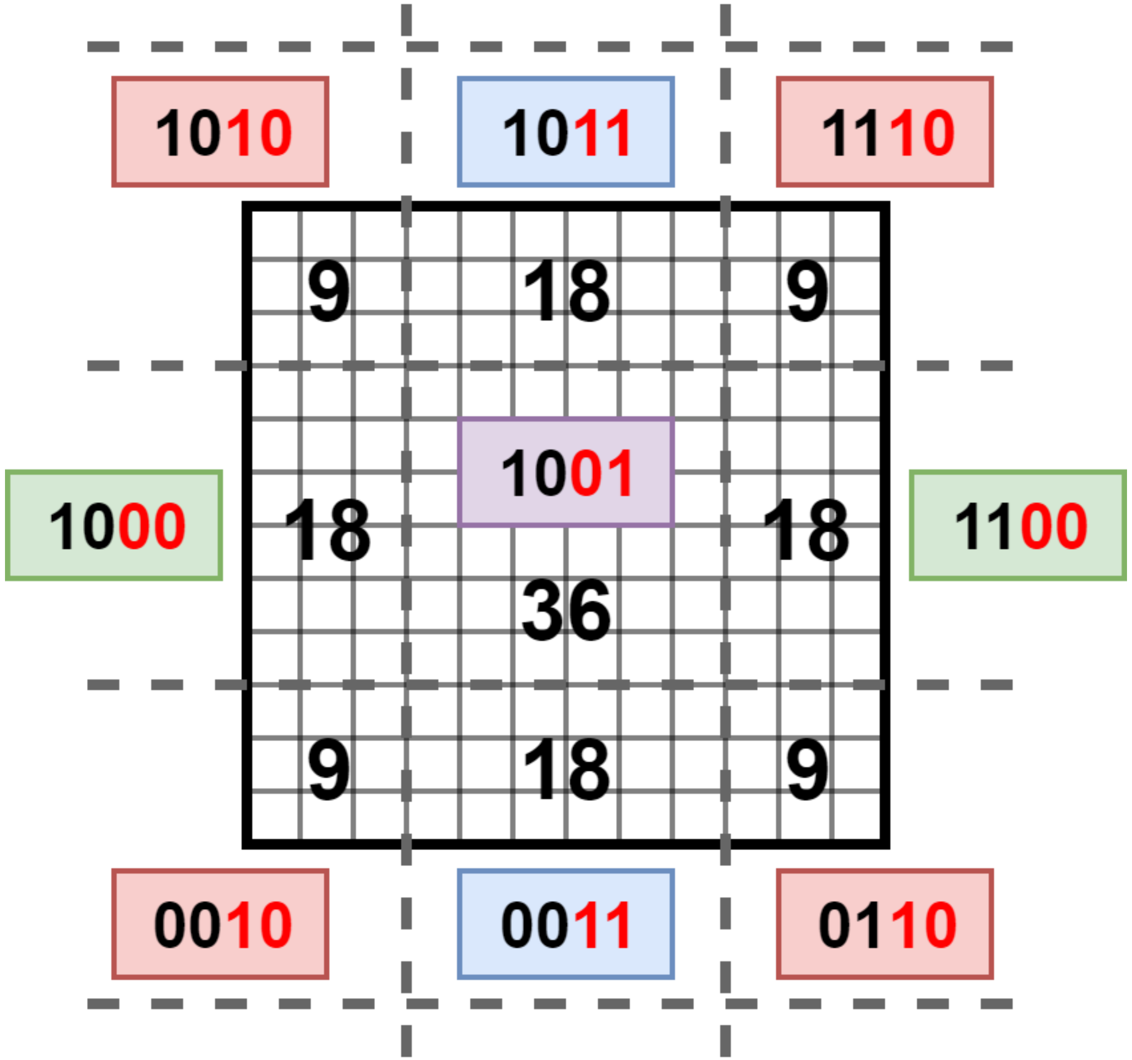
WYNER WIRETAP CODING EXAMPLE



WYNER WIRETAP CODING EXAMPLE

- Eve tries to decode the LSB

Area of 0	Area of 1
4 x 9	2 x 18
+	+
2 x 18	1 x 36
=	=
72	72

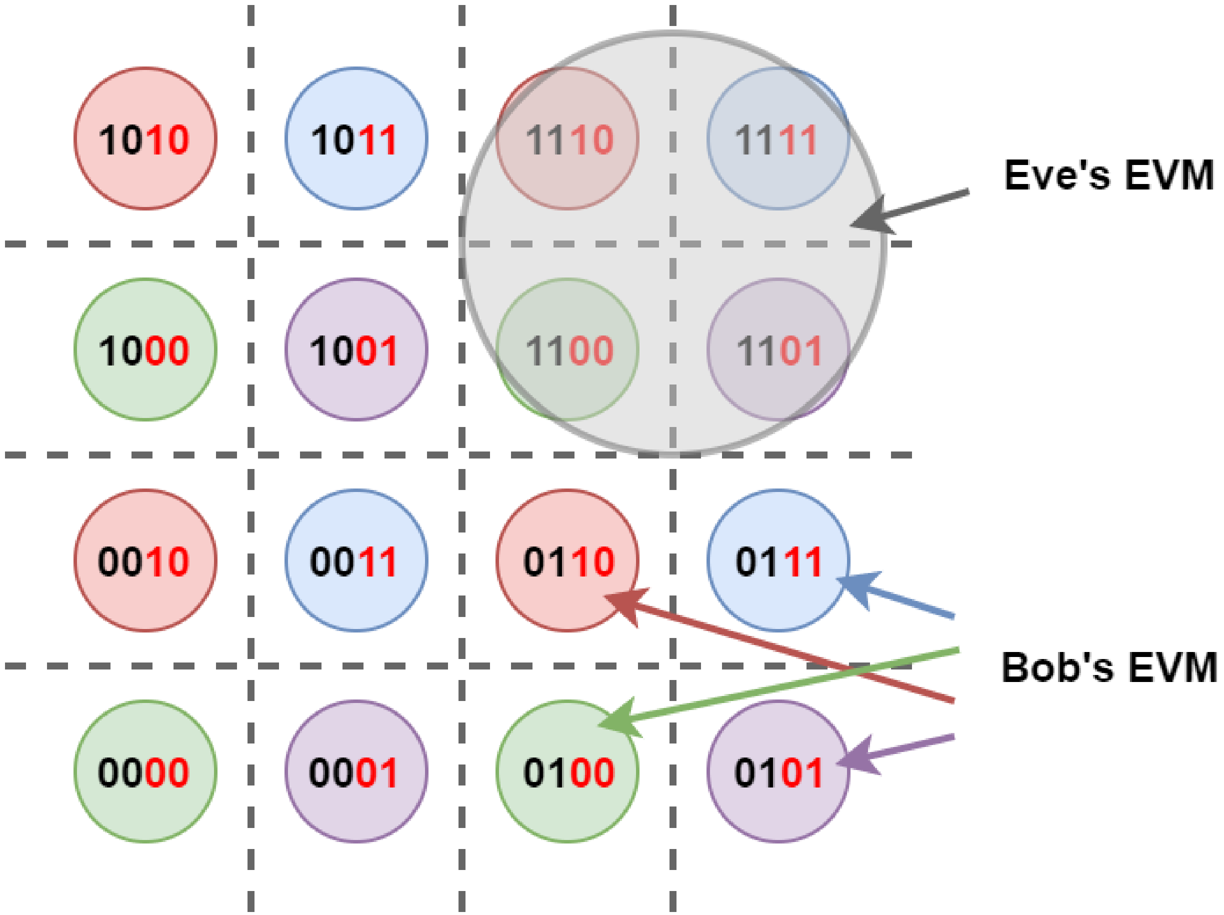


WYNER WIRETAP CODING EXAMPLE

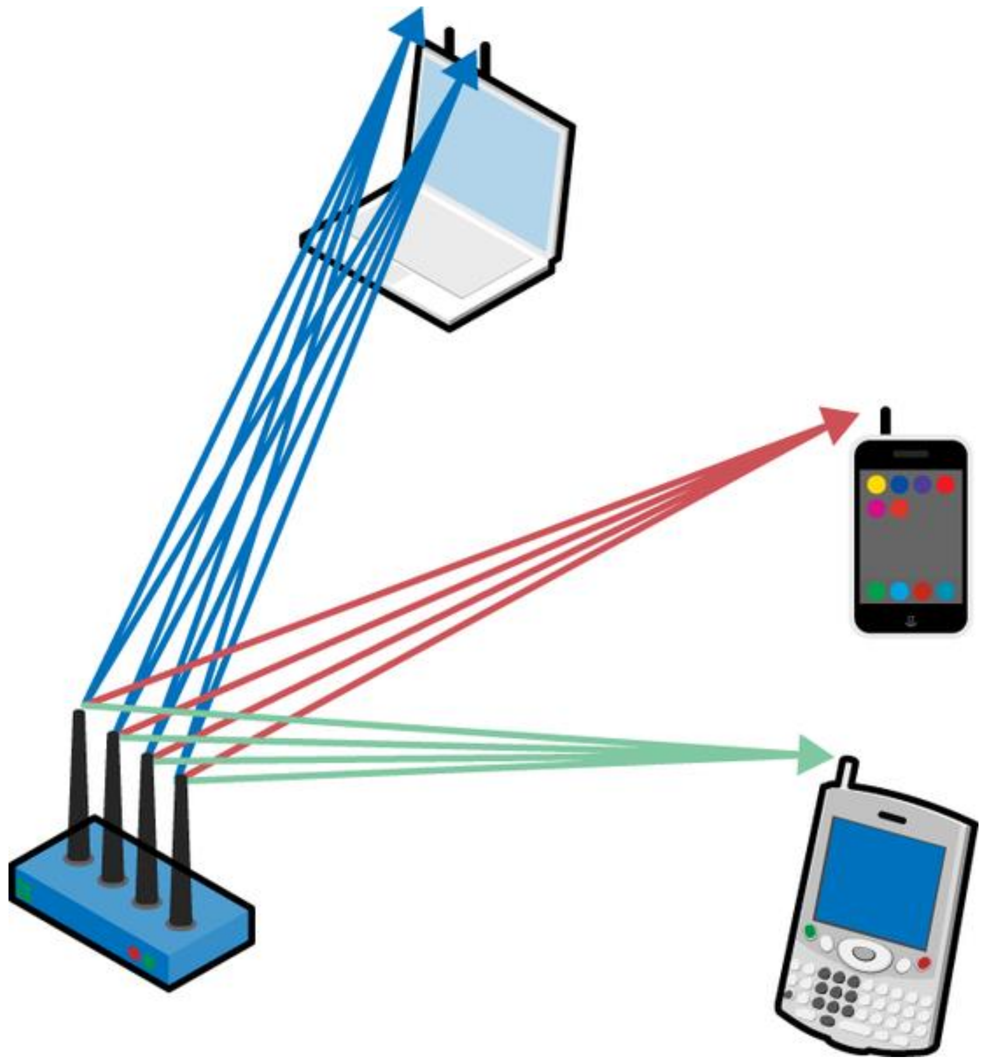
- Bob's Rate (16-QAM) - 4 bits/sym
- Eve's Rate (QPSK) – 2 bits/sym
- Secrecy Rate

$$R_S = R_B - R_E = \underline{\mathbf{2\ bits/sym}}$$

= Protected bit rate



MULTIPLE-INPUT MULTIPLE-OUTPUT COMMUNICATIONS



SINGLE-USER MIMO CHANNEL MODEL

For a single-user MIMO system in **flat fading** with M_T transmit antennas and M_R receive antennas, the received signal is:

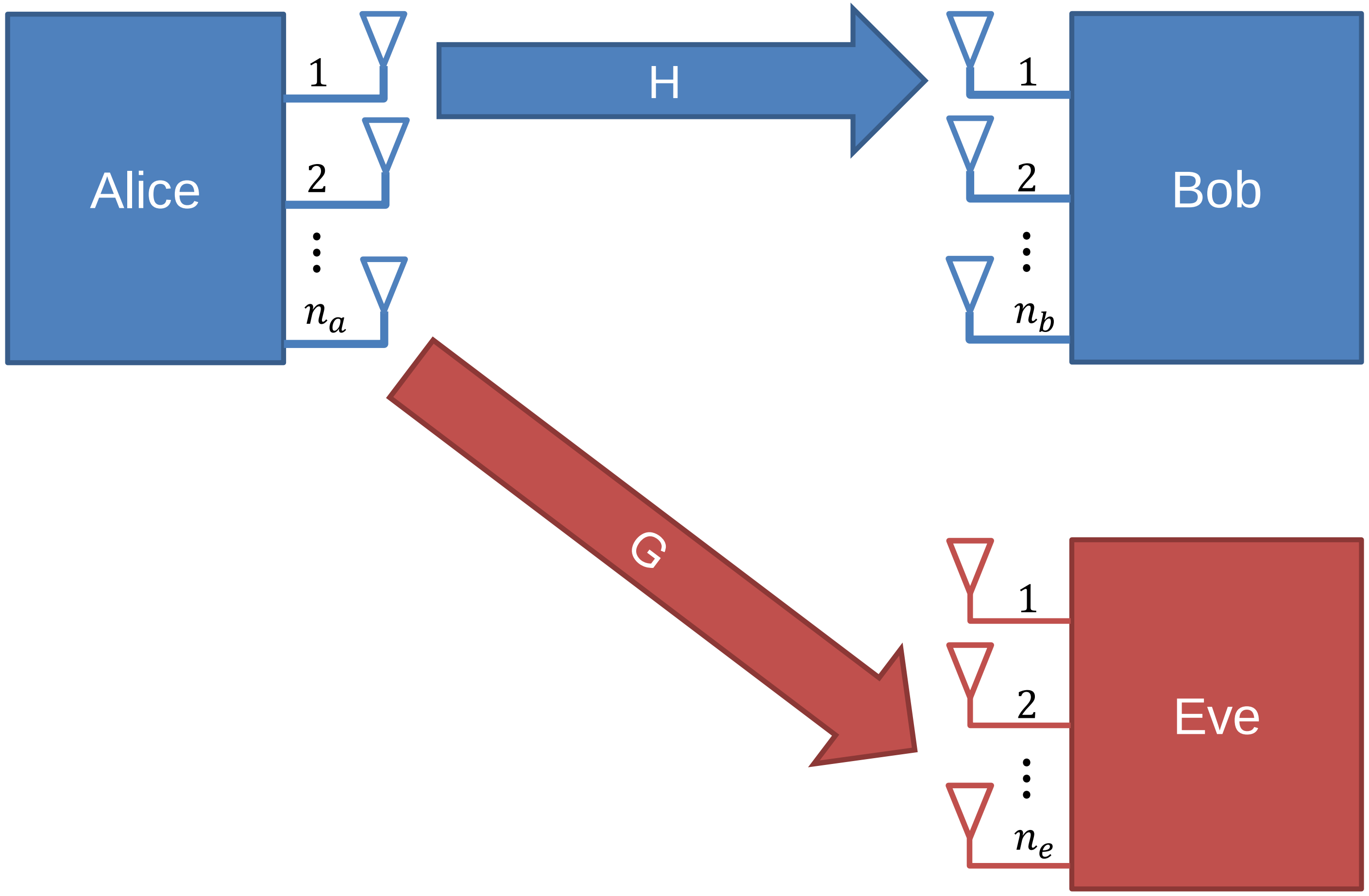
$$\vec{y} = \boldsymbol{H}\vec{x} + \vec{n}$$

Where:

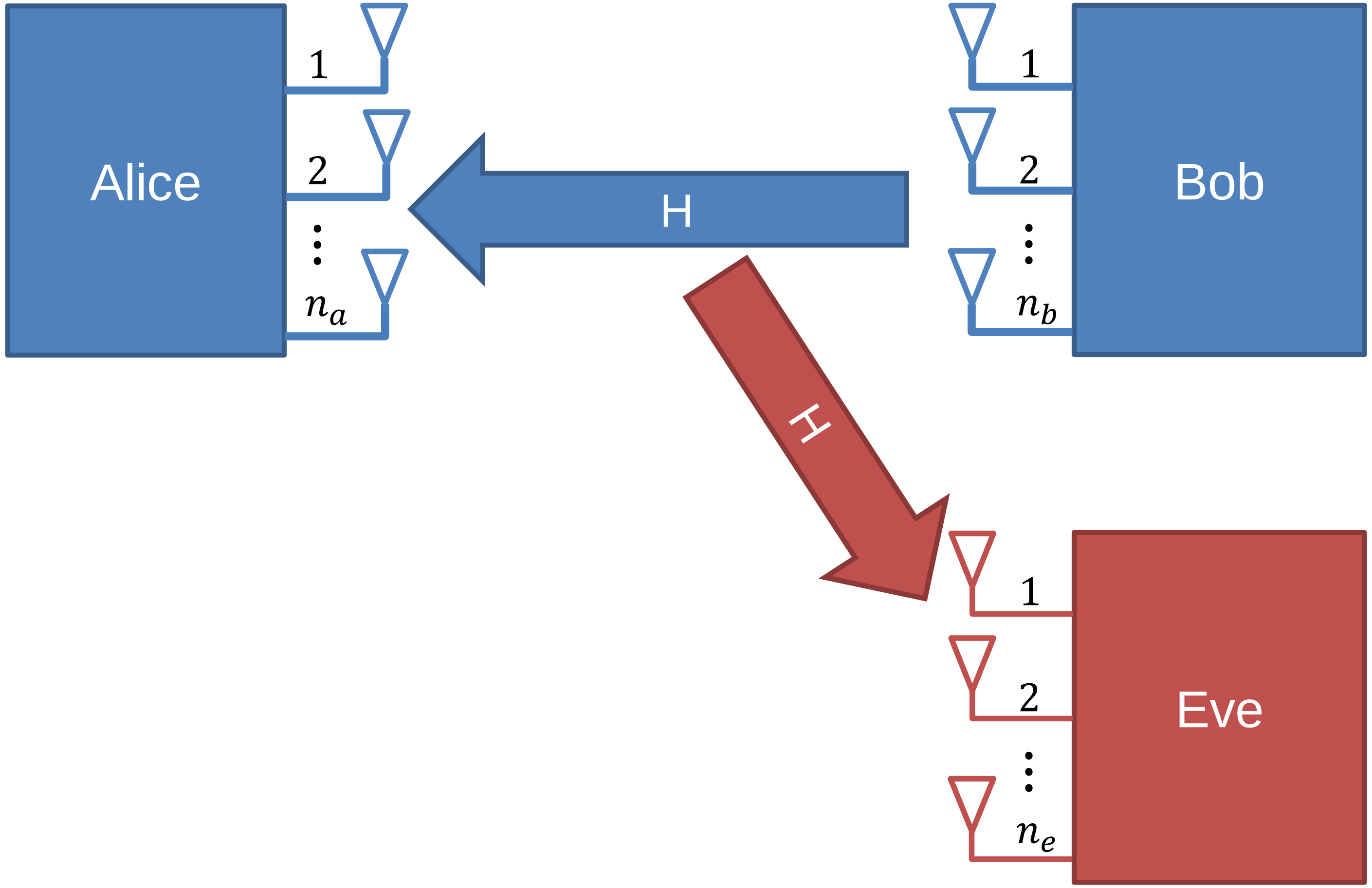
- $\vec{y}$ is the $M_R \times 1$ receive vector
- $\vec{x}$ is the $M_T \times 1$ transmit vector
- $\vec{n}$ is the $M_T \times 1$ noise vector
- $\boldsymbol{H}$ is the $M_R \times M_T$ channel matrix.

$$\boldsymbol{H} = \begin{bmatrix} H_{1,1} & H_{1,2} & \cdots & H_{1,M_T} \\ H_{2,1} & H_{2,2} & \cdots & H_{2,M_T} \\ \vdots & \vdots & \cdots & \cdots \\ H_{M_R,1} & H_{M_R,2} & \cdots & H_{M_R,M_T} \end{bmatrix}$$

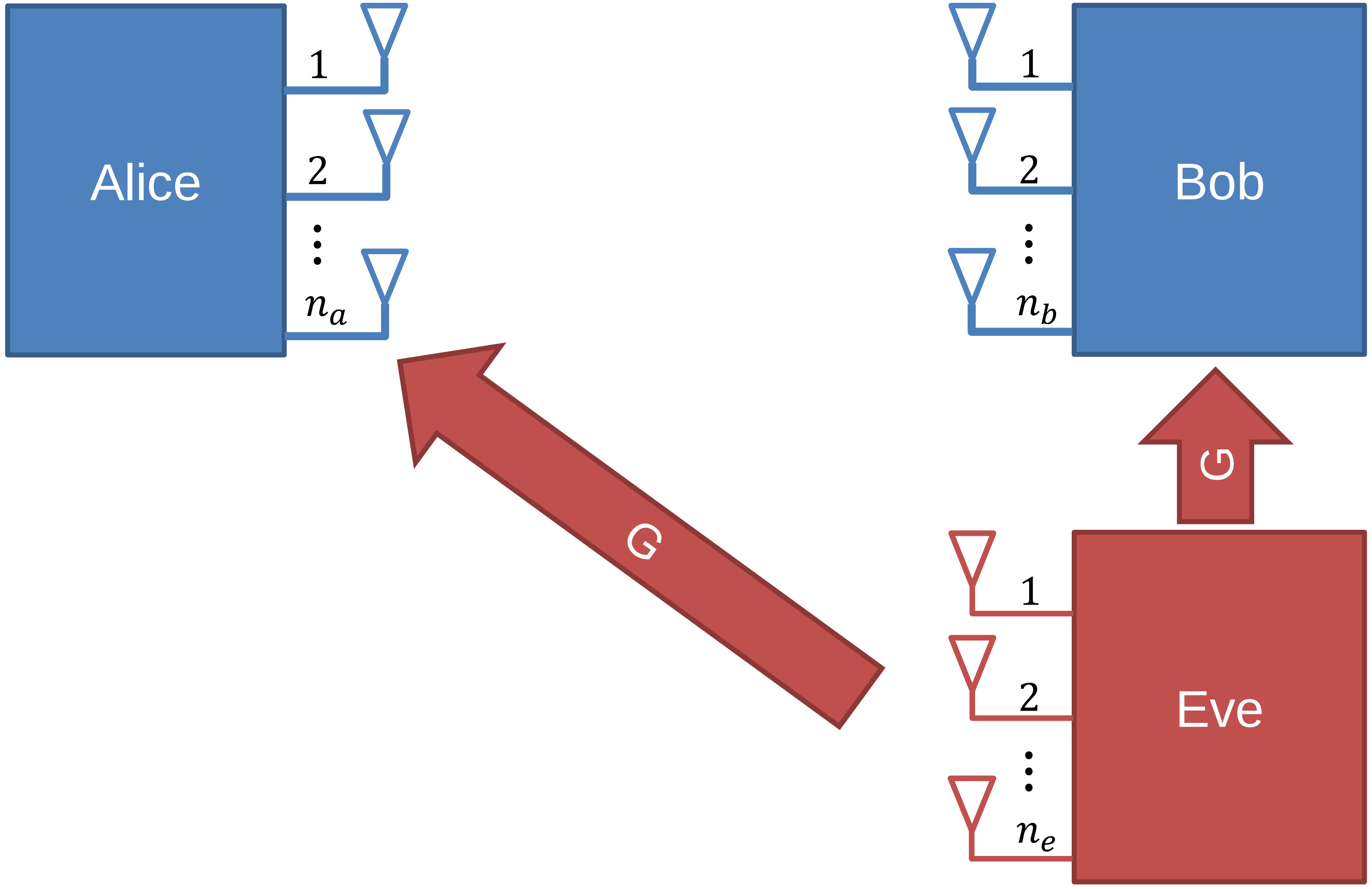
CHANNEL STATE INFORMATION (CSI)



CHANNEL STATE INFORMATION (CSI)



CHANNEL STATE INFORMATION (CSI)



SECRECY MEASURES

Type of Metric	Definition	CSI Requirement
Instantaneous Performance	Secrecy Rate: The rate difference of the legitimate channel and the eavesdropper channel.	Full instantanous CSI or deterministic imperfect CSI
	Secrecy Capacity: The maximum secrecy rate.	
Statistical Performance	Ergodic Secrecy Rate: The statistical average of secrecy rate over channel distributions.	Indeterministic imperfect CSI or statistical CSI
	Secrecy Outage Probability: The probability that the real transmission rate is greater than the secrecy rate.	
	Interception Probability: The probability that the eavesdropper channel rate is great than the secrecy rate.	
Asymptotic Performance	Secrecy Diversity Order: The high-SNR slope of the secrecy outage probability.	
	Secrecy Degrees of Freedom: The number of independent symbols transmitted in parallel at a high SNR.	

Information From: *Xaoming Chen, A Survey on Multiple-Antenna Techniques for Physical Layer Security*

- How we can assess secrecy is fundamentally tied to the CSI available.
- In situations where only statistical knowledge of Bob and/or Eve's channel is available, we will not be able to define a deterministic secrecy rate or capacity and must rely on statistical measures.
- For a passive eavesdropper, we cannot measure secrecy rates!

OVERVIEW

- Intro to Physical Layer Security
- Background Information
- Artificial Noise Generation
- Implementation
- Conclusions and Future Work

Alice transmits

$$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k$$

where $\mathbf{s}_k$ is the source information and $\mathbf{w}_k$ is the AN chosen to lie in the nullspace of $\mathbf{H}_k$ by satisfying

$$\mathbf{H}_k \mathbf{w}_k = 0.$$

The signal received by Bob is

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k$$

$$\mathbf{z}_k = \mathbf{H}_k(\mathbf{s}_k + \mathbf{w}_k) + \mathbf{n}_k$$

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{s}_k + \mathbf{n}_k.$$

The signal received by Eve is

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{x}_k + \mathbf{e}_k$$

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{s}_k + \mathbf{G}_k \mathbf{w}_k + \mathbf{e}_k$$

where the $\mathbf{G}_k \mathbf{w}_k$ represents the additional noise seen by Eve.

Alice transmits

$$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k$$

where $\mathbf{s}_k$ is the source information and $\mathbf{w}_k$ is the AN chosen to lie in the nullspace of $\mathbf{H}_k$ by satisfying

$$\boxed{\mathbf{H}_k \mathbf{w}_k = 0.}$$

The signal received by Bob is

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k$$

$$\mathbf{z}_k = \mathbf{H}_k (\mathbf{s}_k + \mathbf{w}_k) + \mathbf{n}_k$$

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{s}_k + \mathbf{n}_k.$$

The signal received by Eve is

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{x}_k + \mathbf{e}_k$$

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{s}_k + \mathbf{G}_k \mathbf{w}_k + \mathbf{e}_k$$

where the $\mathbf{G}_k \mathbf{w}_k$ represents the additional noise seen by Eve.

Alice transmits

$$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k$$

where $\mathbf{s}_k$ is the source information and $\mathbf{w}_k$ is the AN chosen to lie in the nullspace of $\mathbf{H}_k$ by satisfying

$$\mathbf{H}_k\mathbf{w}_k = 0.$$

The signal received by Bob is

$$\mathbf{z}_k = \mathbf{H}_k\mathbf{x}_k + \mathbf{n}_k$$

$$\mathbf{z}_k = \mathbf{H}_k(\mathbf{s}_k + \mathbf{w}_k) + \mathbf{n}_k$$

$$\boxed{\mathbf{z}_k = \mathbf{H}_k\mathbf{s}_k + \mathbf{n}_k.}$$

The signal received by Eve is

$$\mathbf{y}_k = \mathbf{G}_k\mathbf{x}_k + \mathbf{e}_k$$

$$\boxed{\mathbf{y}_k = \mathbf{G}_k\mathbf{s}_k + \mathbf{G}_k\mathbf{w}_k + \mathbf{e}_k}$$

where the $\mathbf{G}_k\mathbf{w}_k$ represents the additional noise seen by Eve.

Alice transmits

$$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k$$

where $\mathbf{s}_k$ is the source information and $\mathbf{w}_k$ is the AN chosen to lie in the nullspace of $\mathbf{H}_k$ by satisfying

$$\mathbf{H}_k \mathbf{w}_k = 0.$$

The signal received by Bob is

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k$$

$$\mathbf{z}_k = \mathbf{H}_k (\mathbf{s}_k + \mathbf{w}_k) + \mathbf{n}_k$$

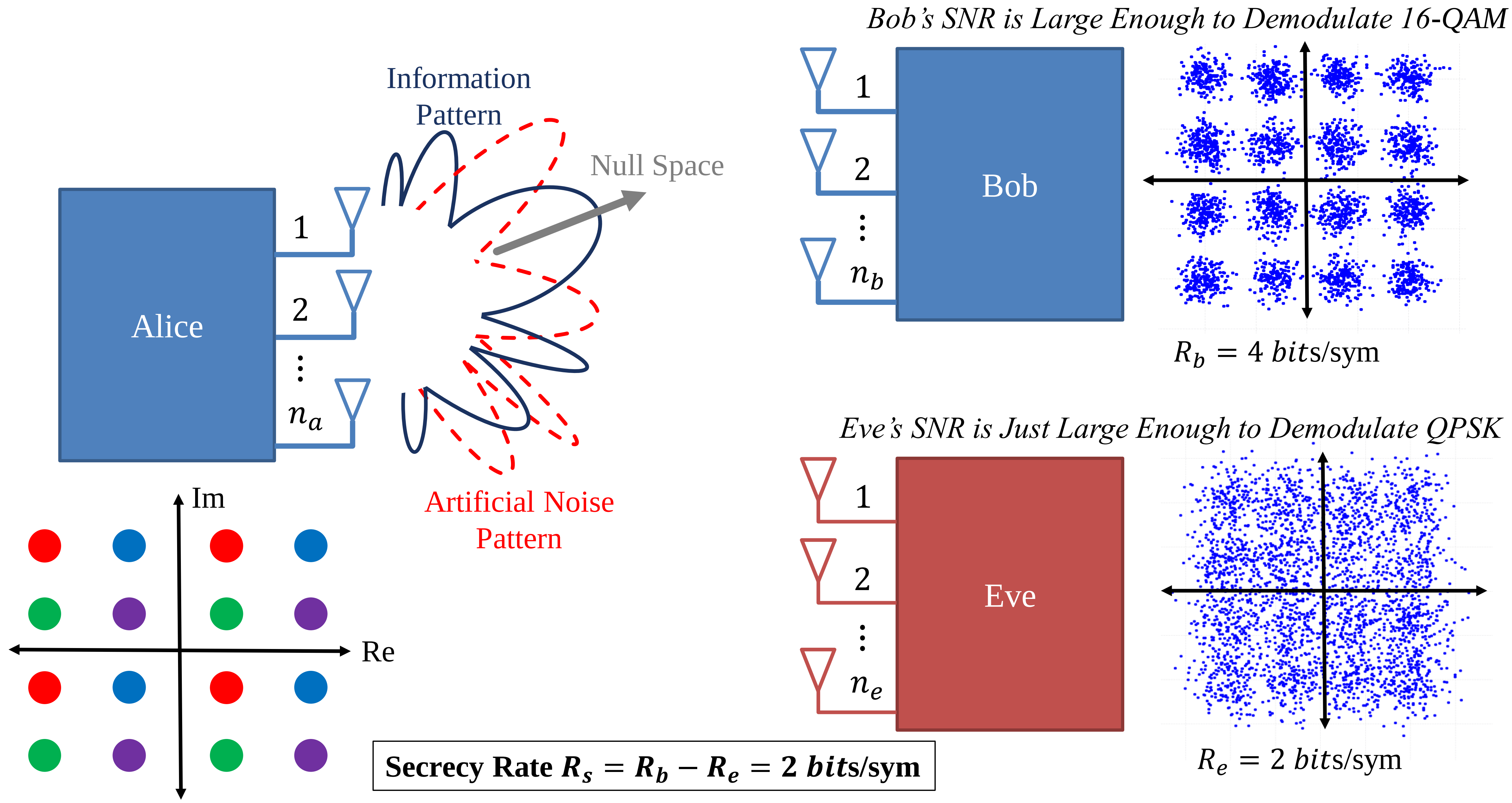
$$\mathbf{z}_k = \mathbf{H}_k \mathbf{s}_k + \mathbf{n}_k.$$

The signal received by Eve is

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{x}_k + \mathbf{e}_k$$

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{s}_k + \boxed{\mathbf{G}_k \mathbf{w}_k} + \mathbf{e}_k$$

where the $\mathbf{G}_k \mathbf{w}_k$ represents the additional noise seen by Eve.

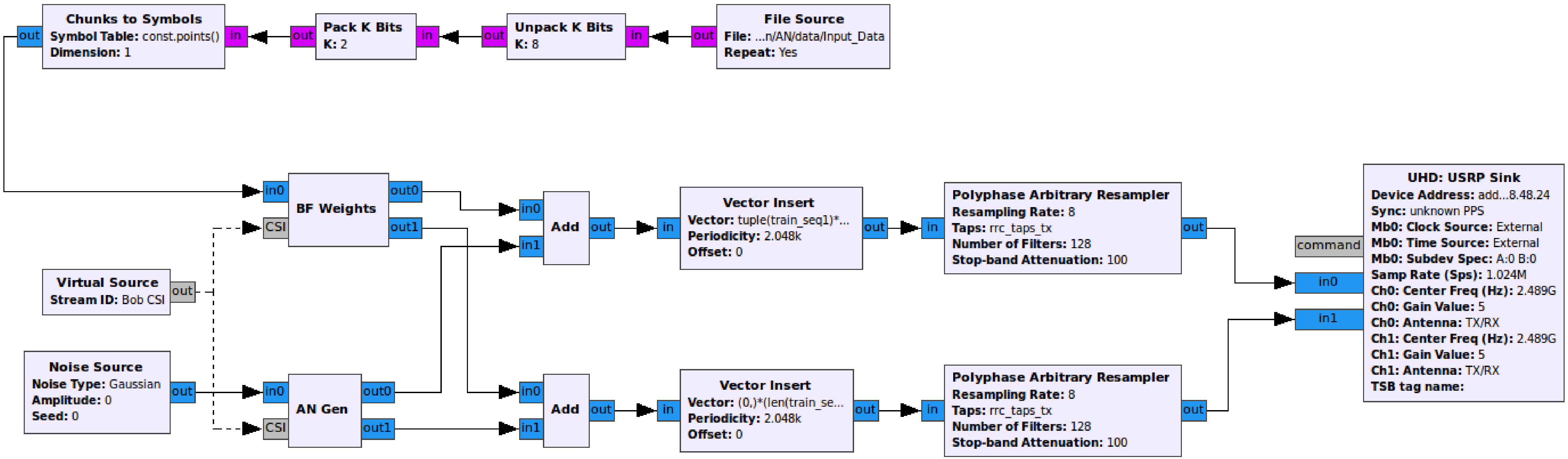


Bob's SNR is Large Enough to Demodulate 16-QAM
Information Pattern
Null Space
1
2
n_b
Bob
$R_b = 4$ bits/sym
Alice
1
2
n_a
Im
Re
Artificial Noise Pattern
Eve's SNR is Just Large Enough to Demodulate QPSK
1
2
n_e
Eve
$R_e = 2$ bits/sym
Secrecy Rate $R_s = R_b - R_e = 2$ bits/sym

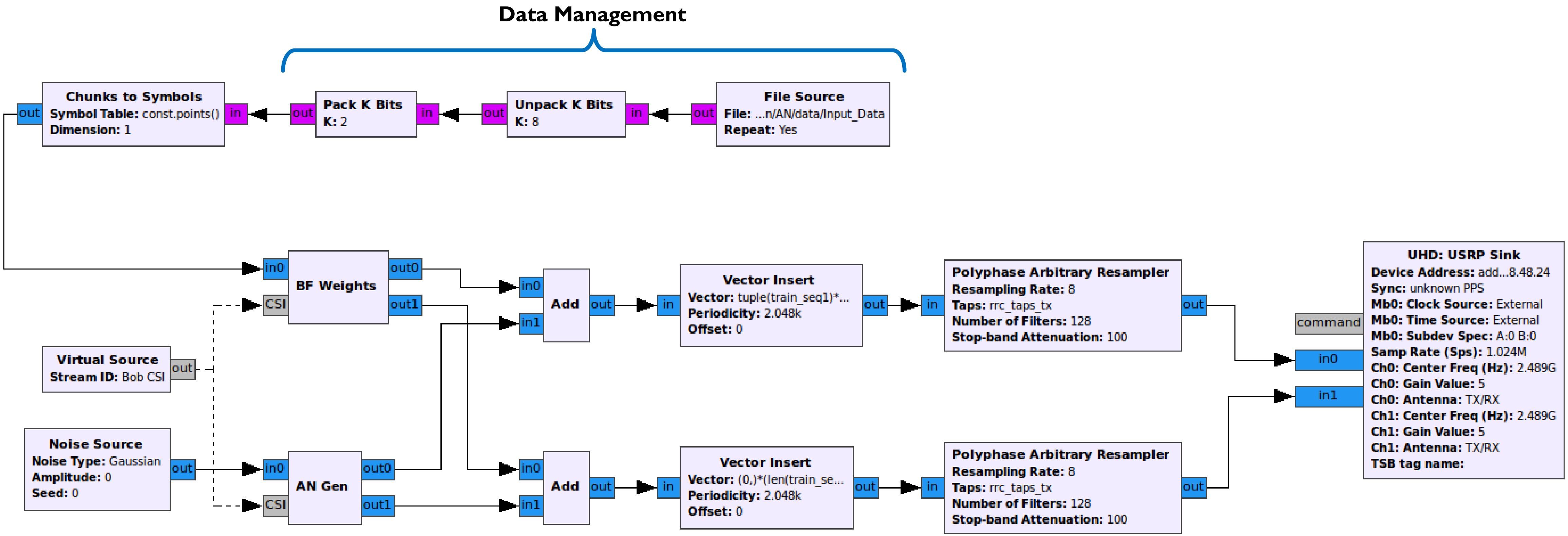
OVERVIEW

- Intro to Physical Layer Security
- Background Information
- Artificial Noise Generation
- Implementation
- Ongoing and Future Work

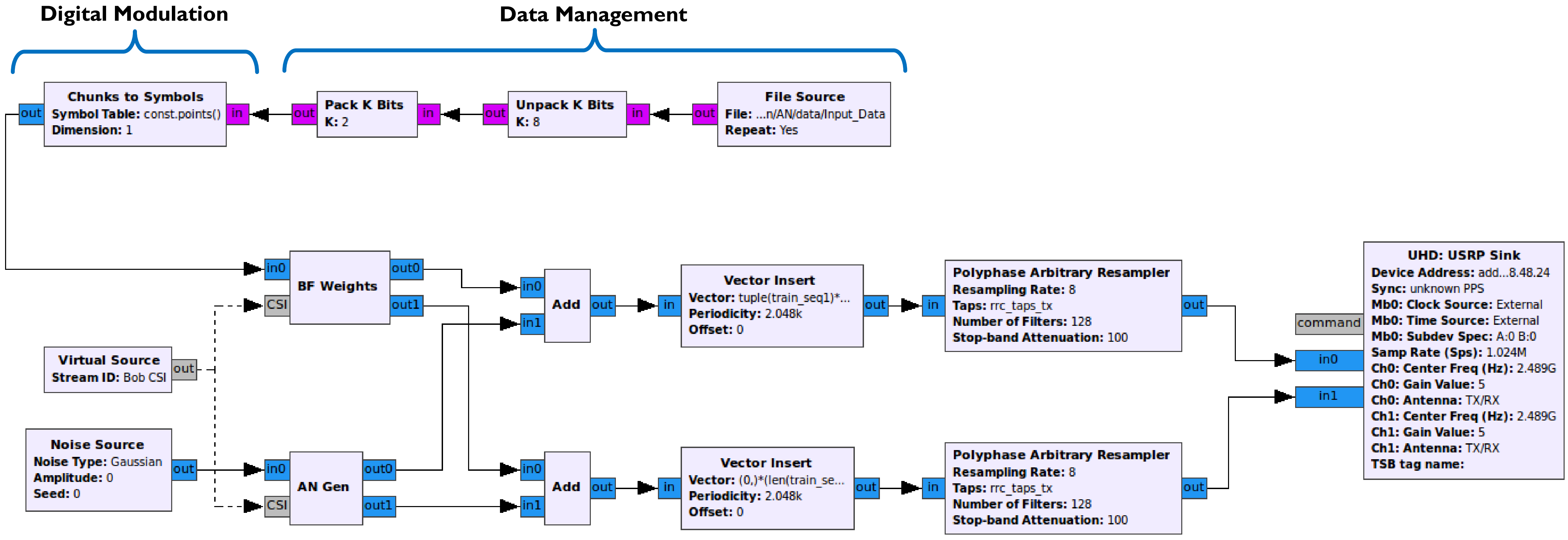
ARTIFICIAL NOISE TRANSMITTER



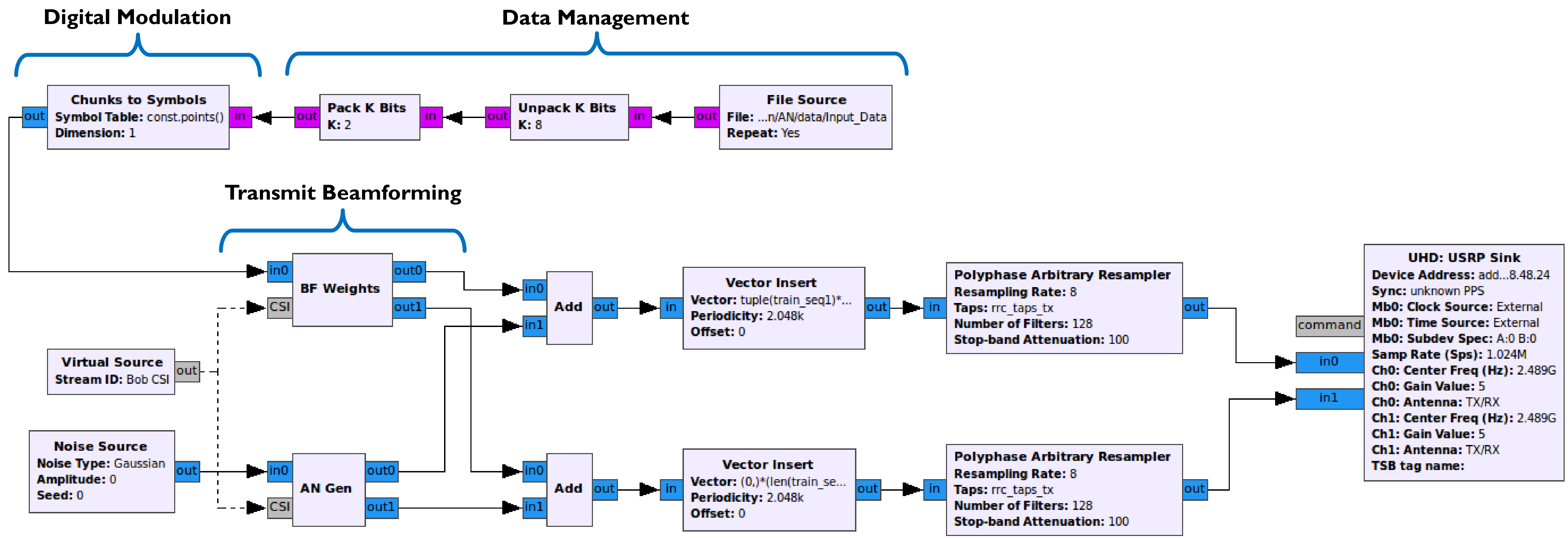
ARTIFICIAL NOISE TRANSMITTER



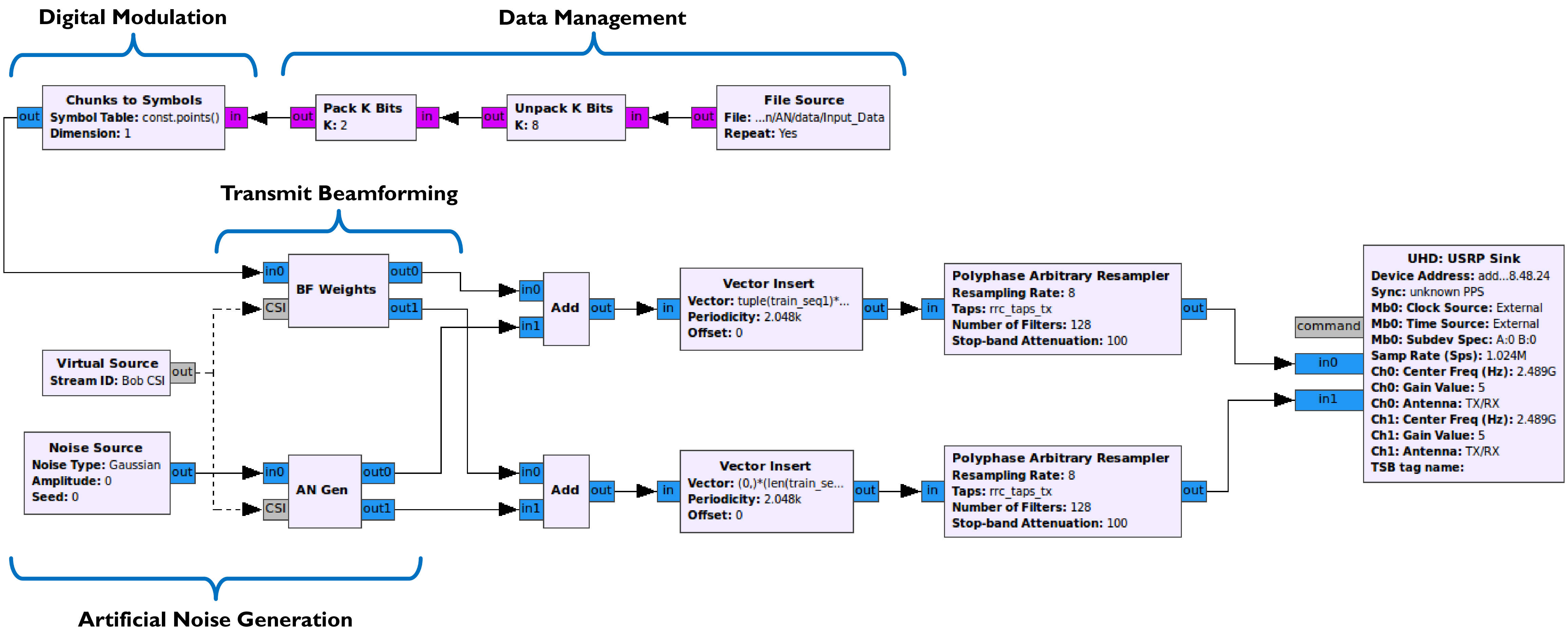
ARTIFICIAL NOISE TRANSMITTER



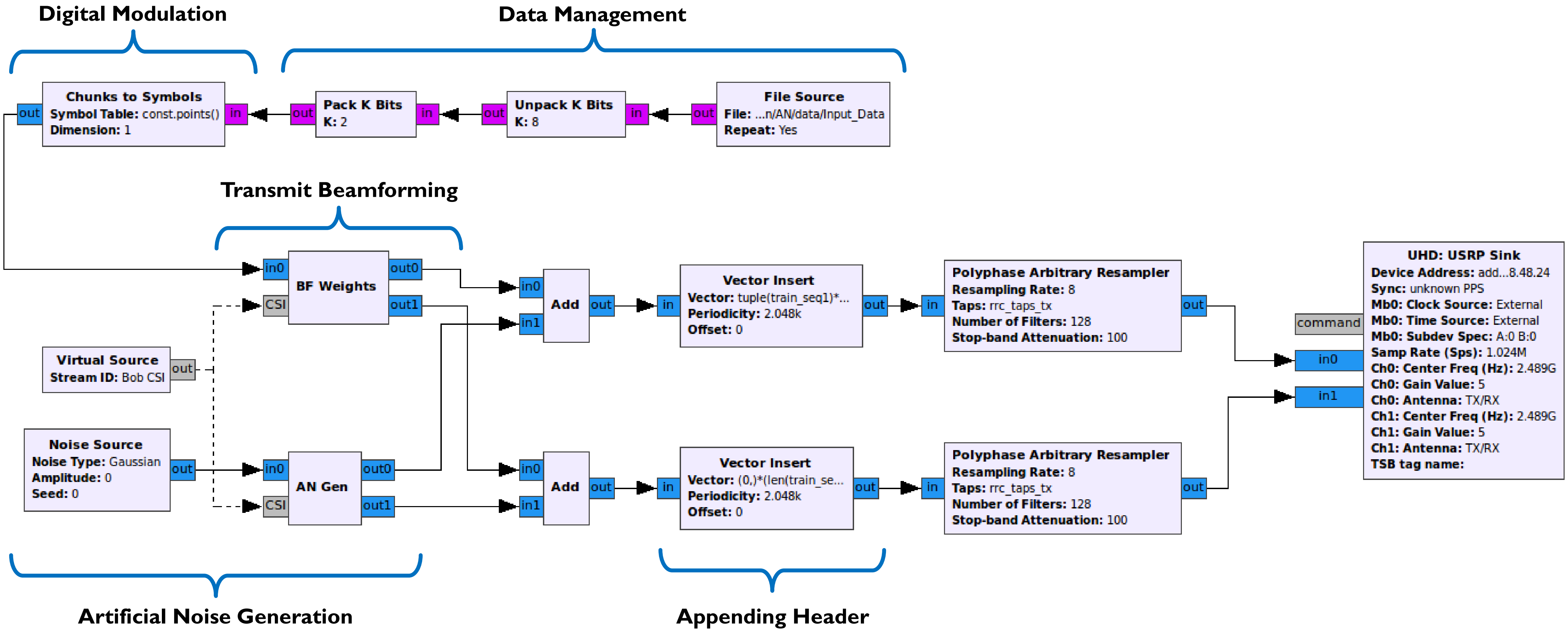
ARTIFICIAL NOISE TRANSMITTER



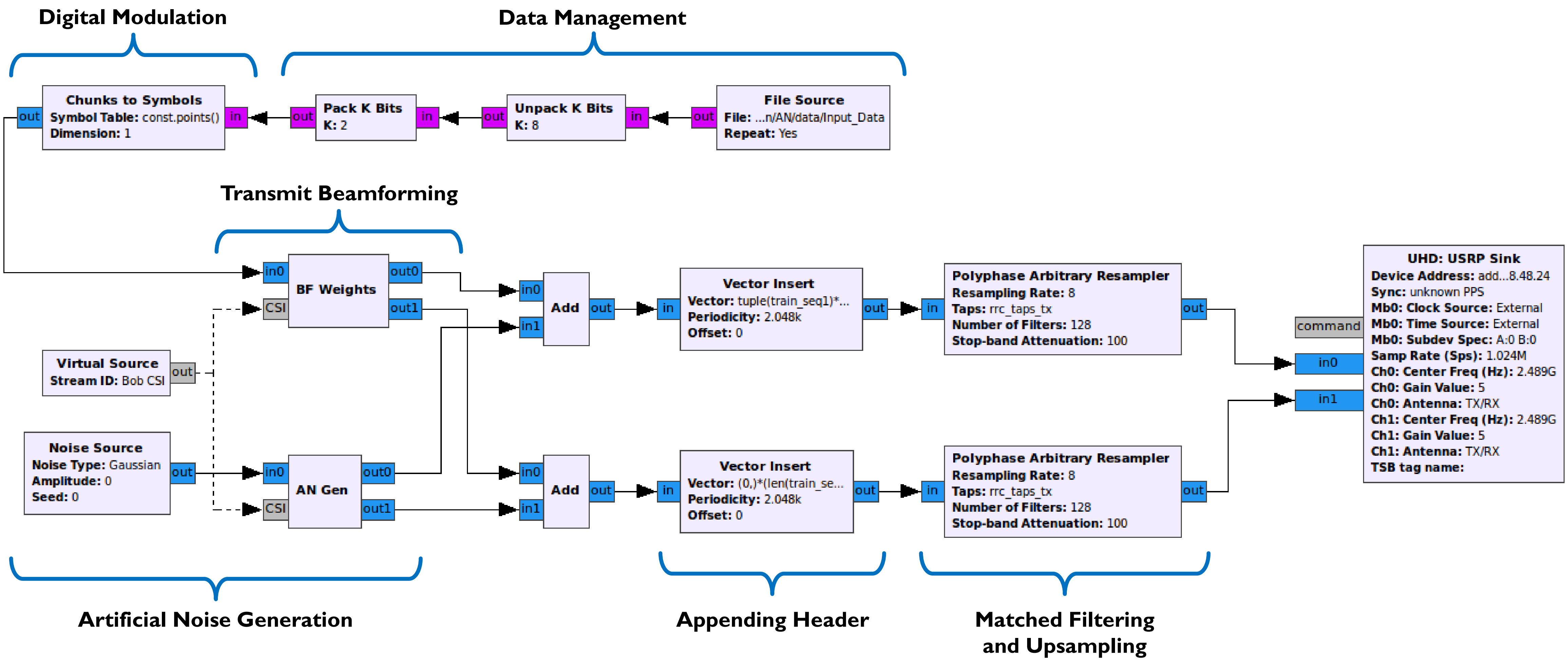
ARTIFICIAL NOISE TRANSMITTER



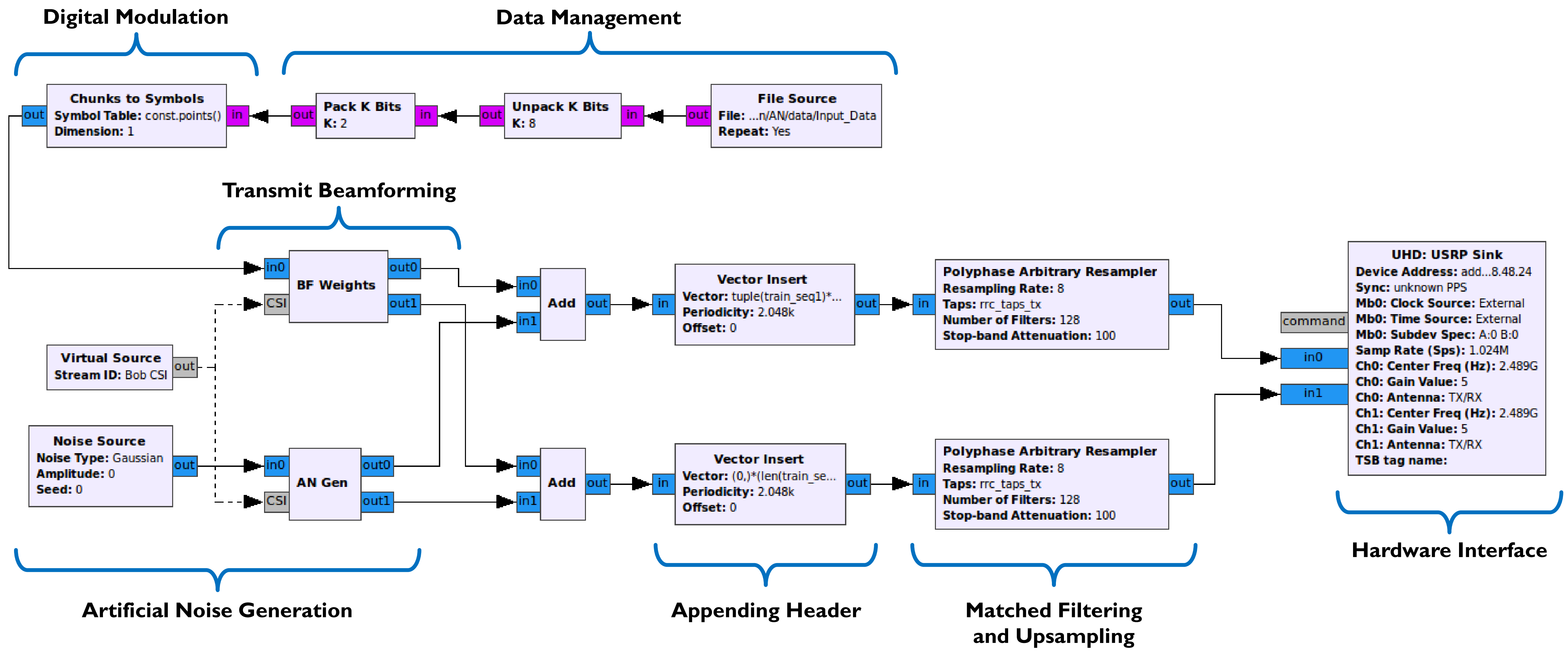
ARTIFICIAL NOISE TRANSMITTER



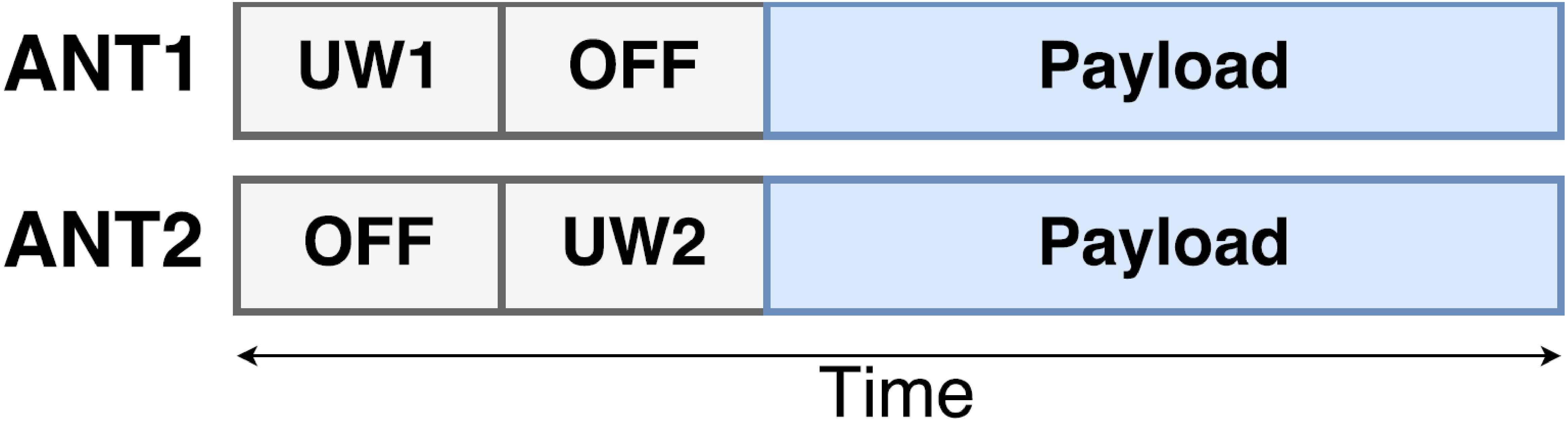
ARTIFICIAL NOISE TRANSMITTER



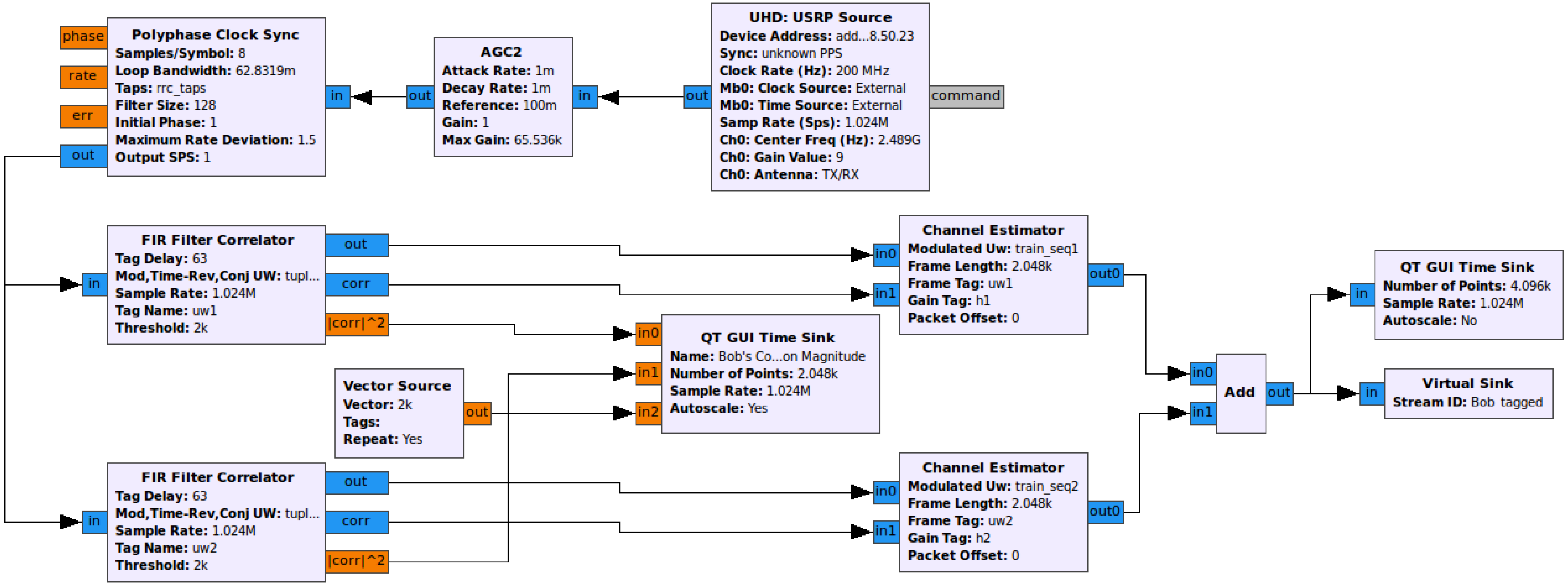
ARTIFICIAL NOISE TRANSMITTER



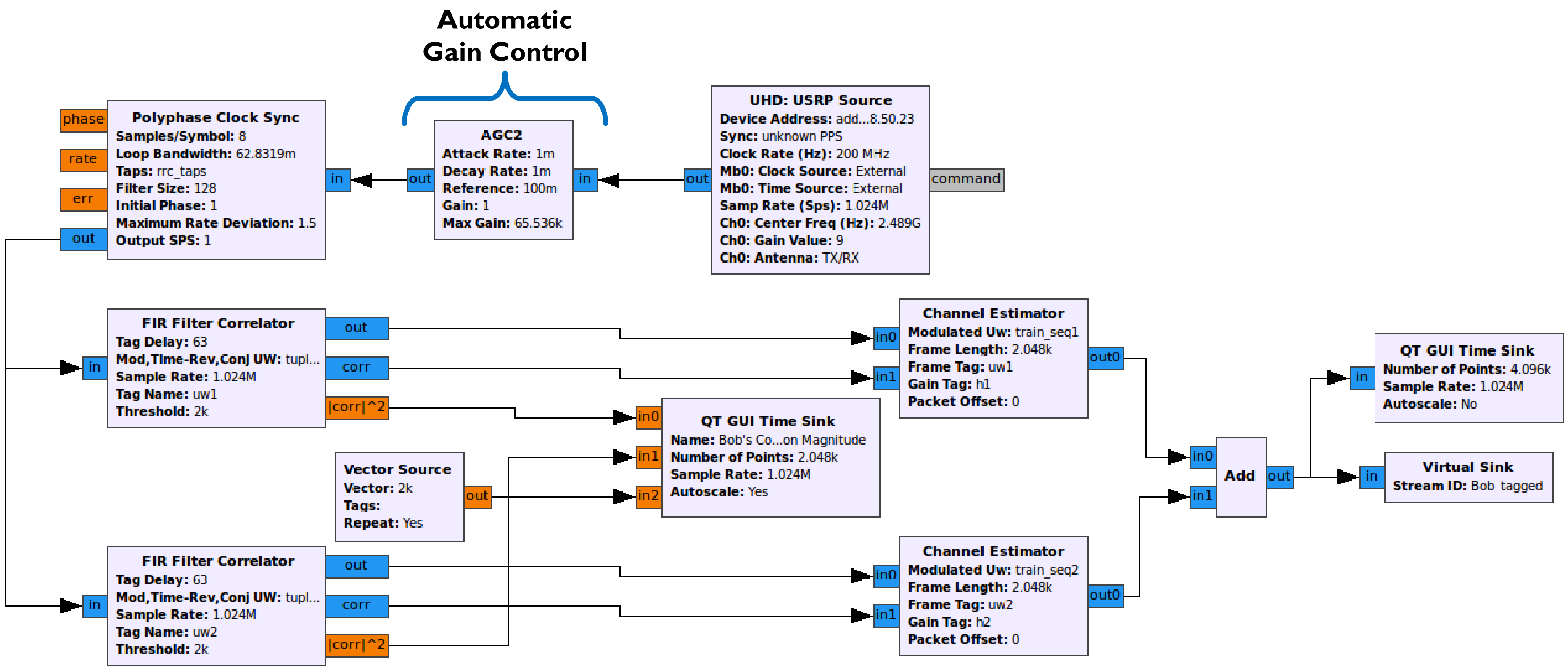
HEADER DESIGN



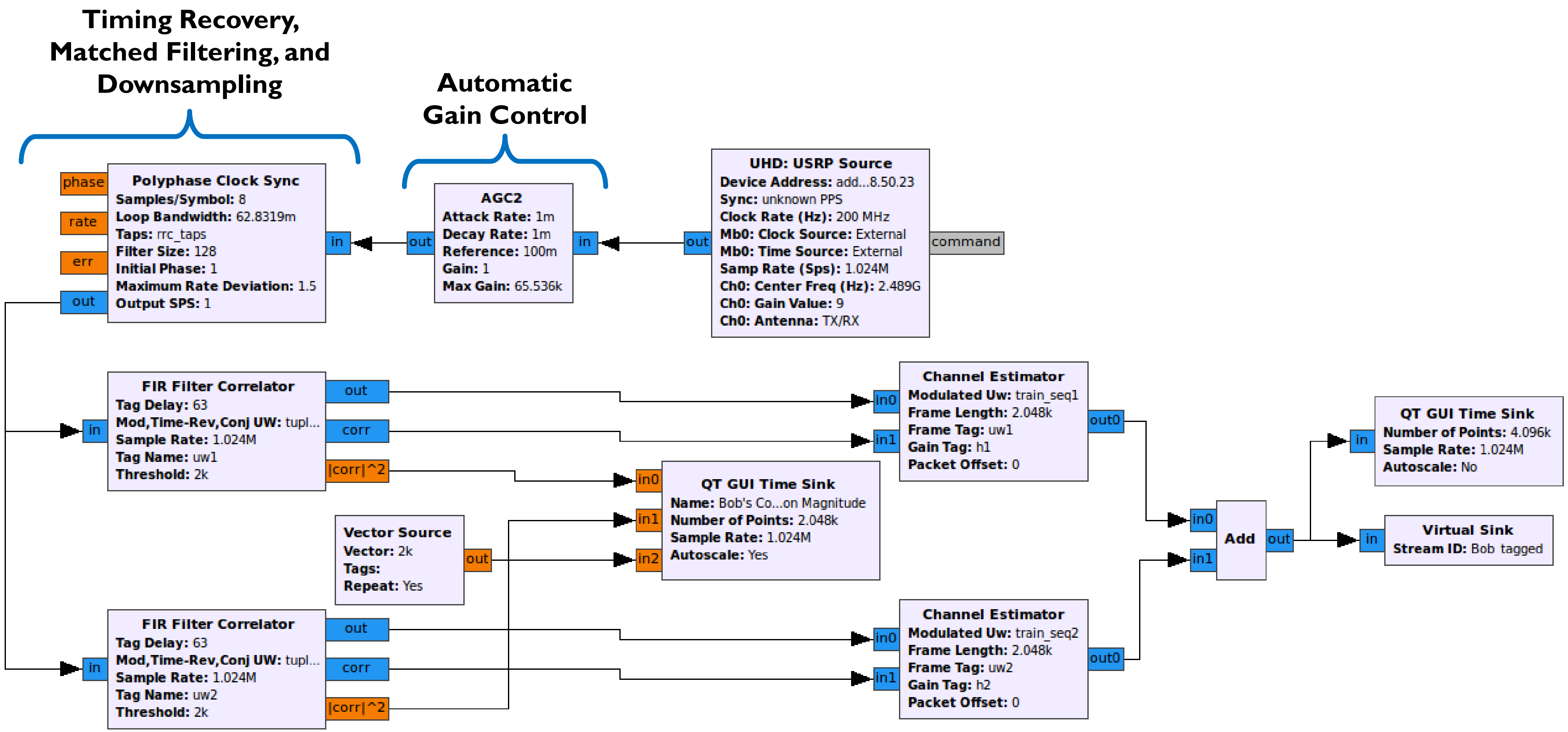
BOB'S ARTIFICIAL NOISE RECEIVER PART 1



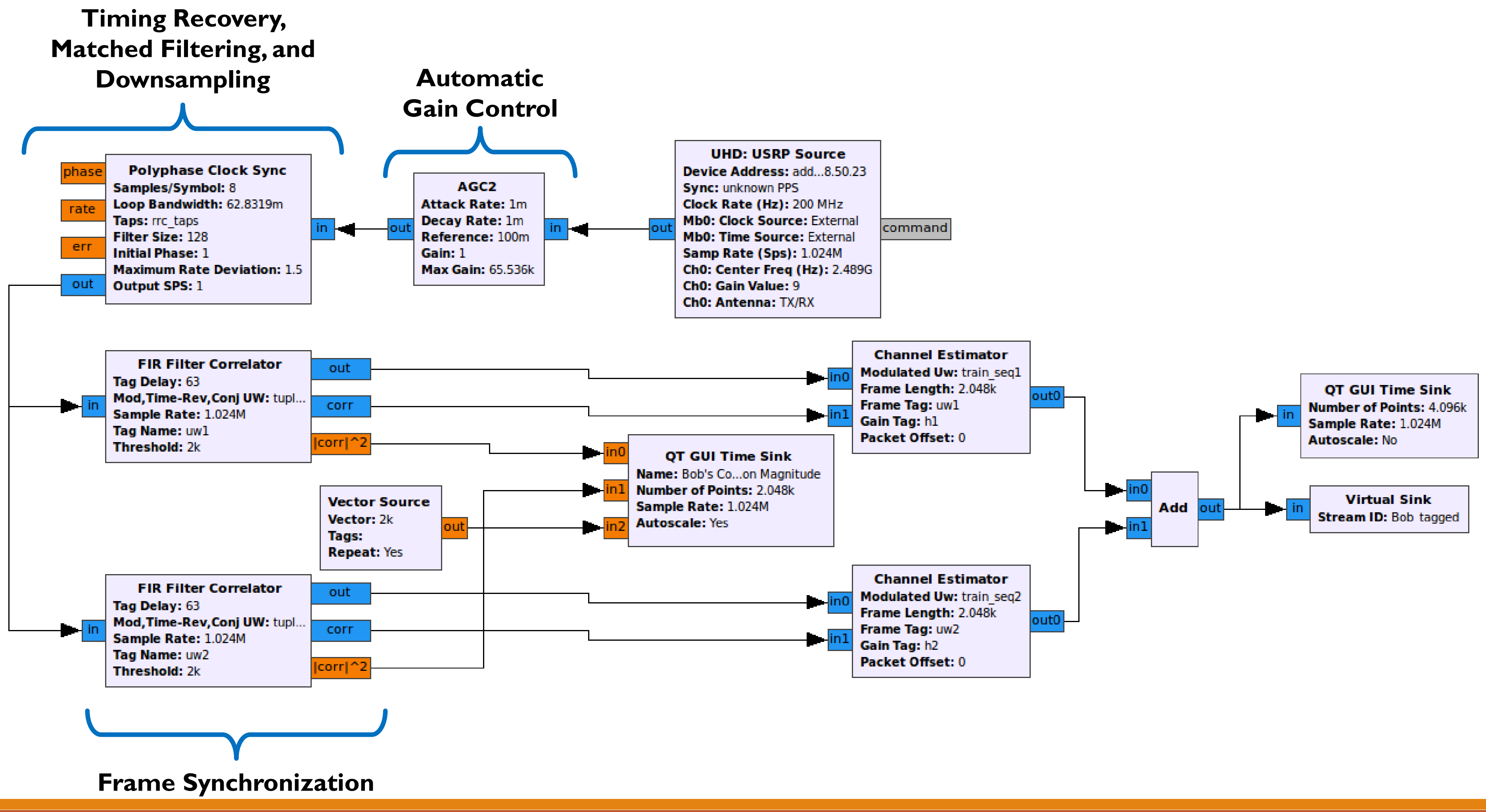
BOB'S ARTIFICIAL NOISE RECEIVER PART I



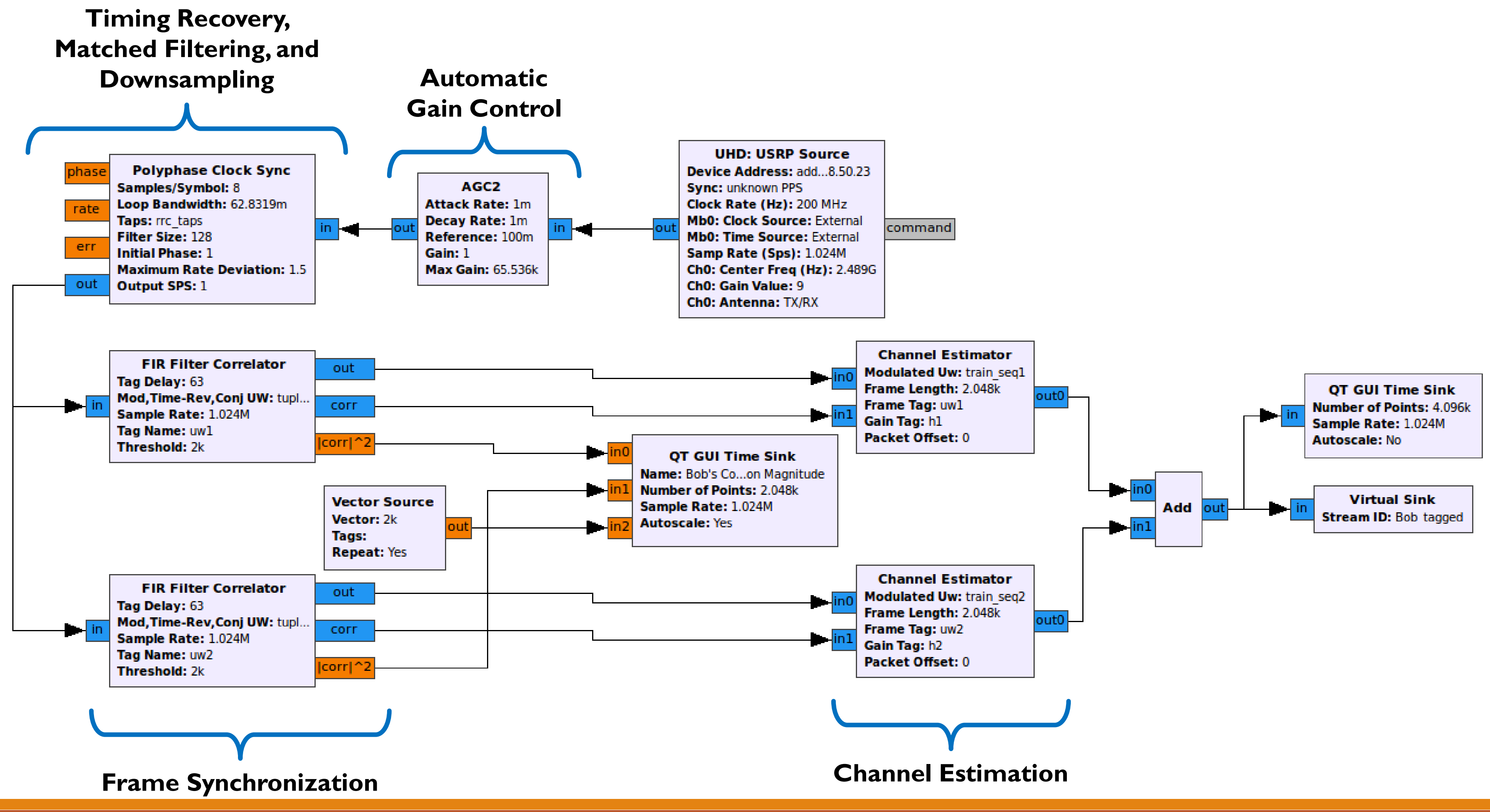
BOB'S ARTIFICIAL NOISE RECEIVER PART 1



BOB'S ARTIFICIAL NOISE RECEIVER PART 1



BOB'S ARTIFICIAL NOISE RECEIVER PART I



The discrete complex cross-correlation of two sequences $p[n]$ and $u[n]$ of length N is defined as

$$R(p,u) = \sum_{m=0}^{N-1} p[m]u^*[m-n].$$

A FIR filter of order $N-1$ performs a convolution operation of the input $x[n]$ with the filter taps $h[n]$ to produce the output

$$y[n] = \sum_{m=0}^{N-1} x[m]h[n-m]$$

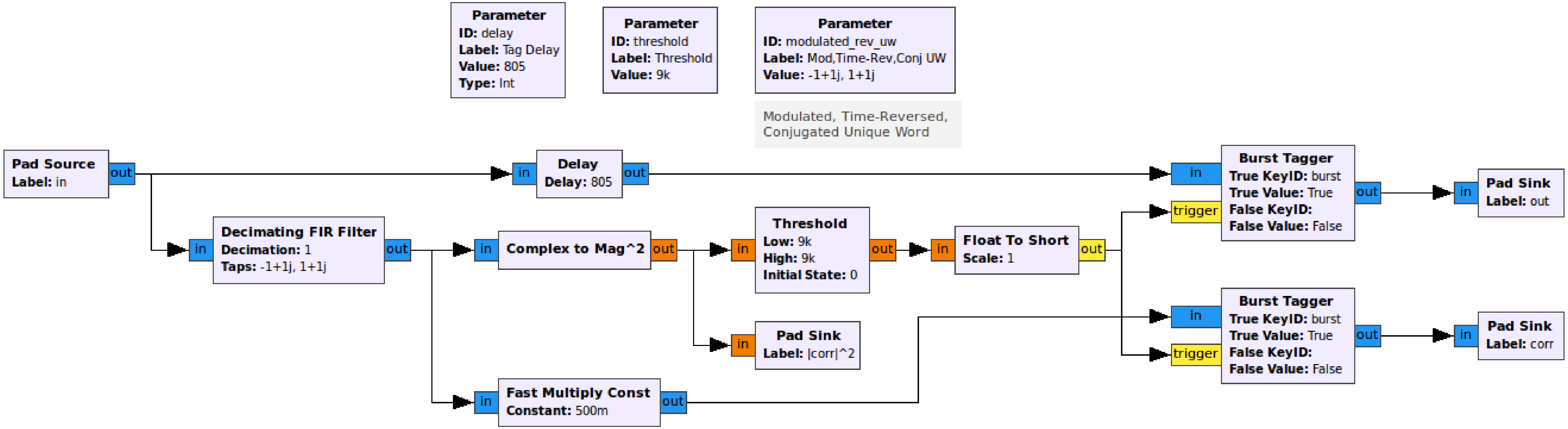
By substituting the taps

$$h_{corr}[n] = u^*[-n]$$

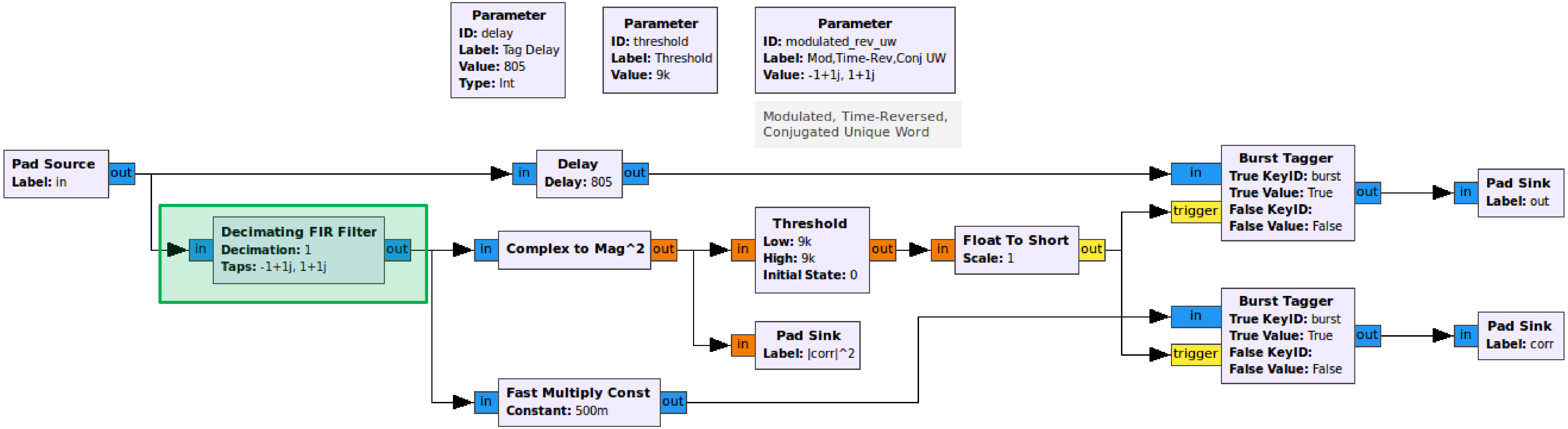
into the FIR filter, the output becomes

$$y_{corr}[n] = \sum_{m=0}^{N-1} x[m]u^*[m-n] = R(x,u)$$

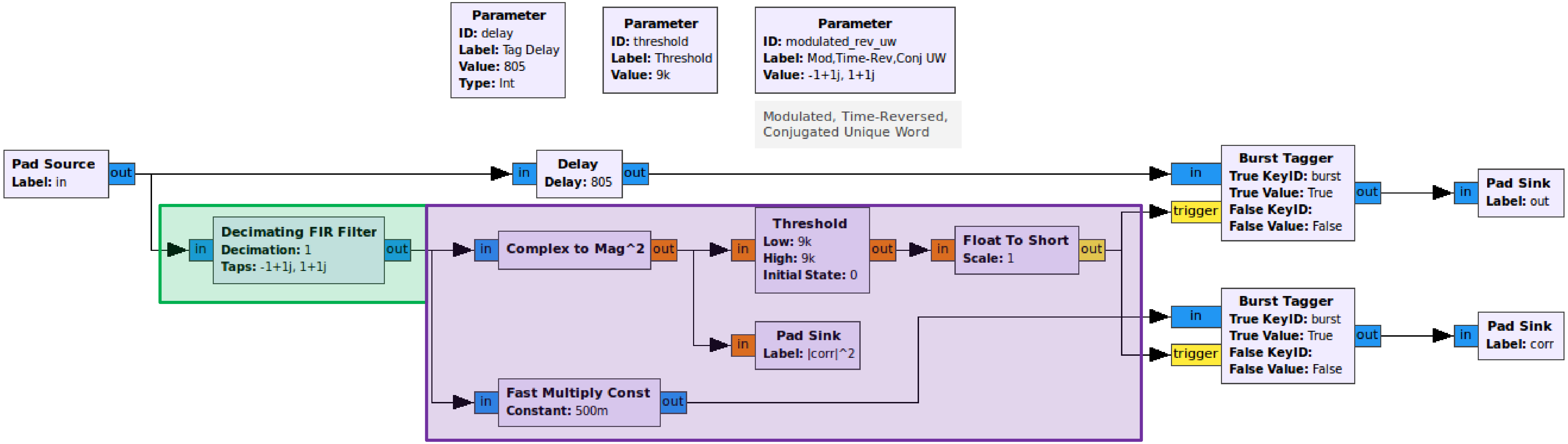
FIR FILTER CORRELATOR



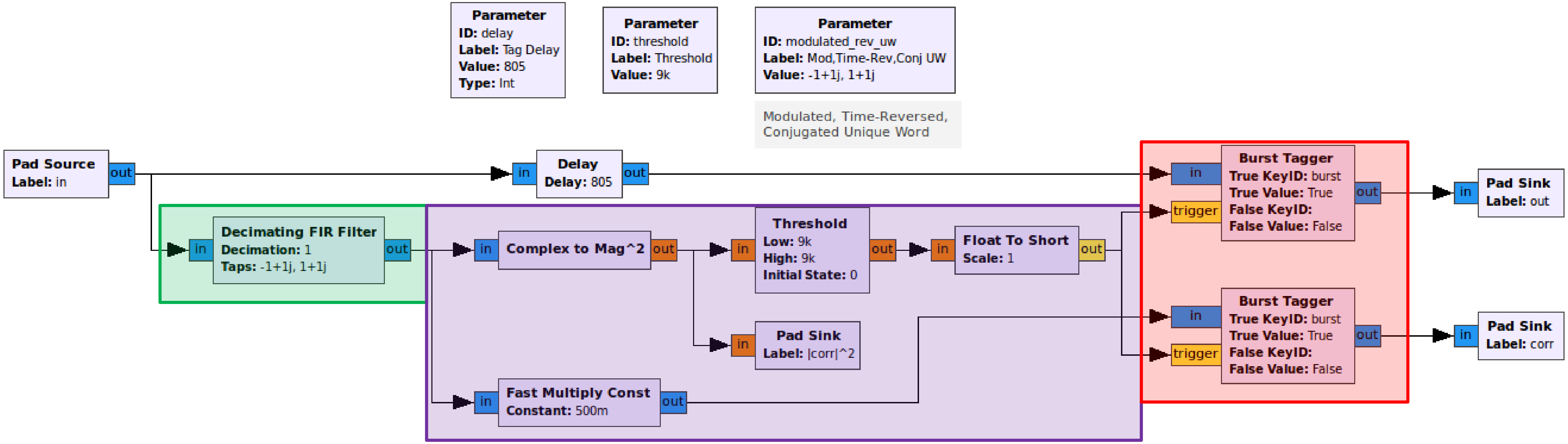
FIR FILTER CORRELATOR



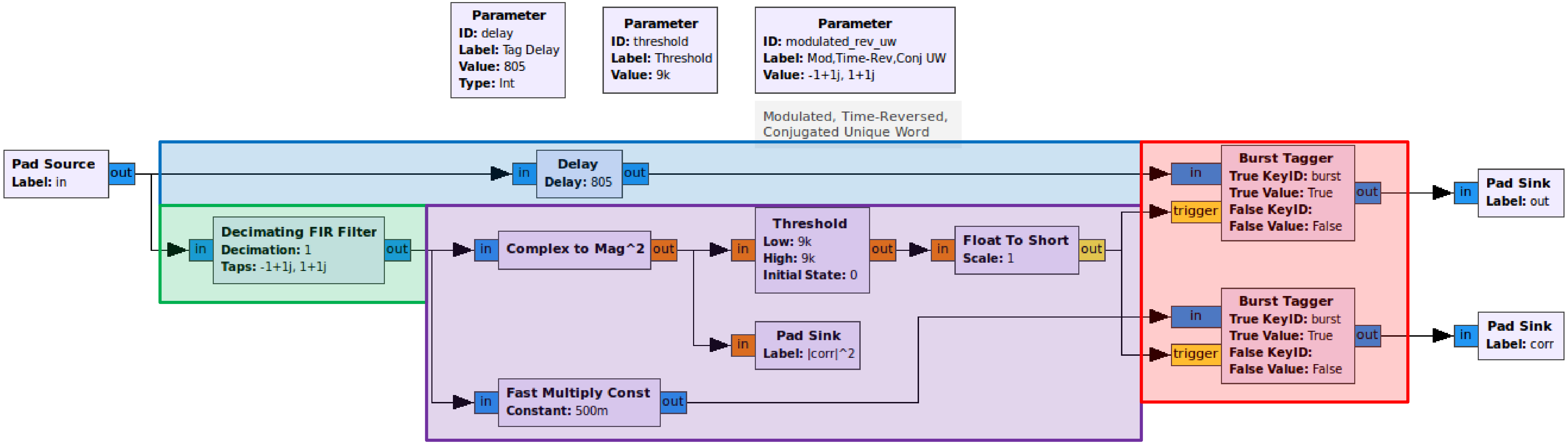
FIR FILTER CORRELATOR



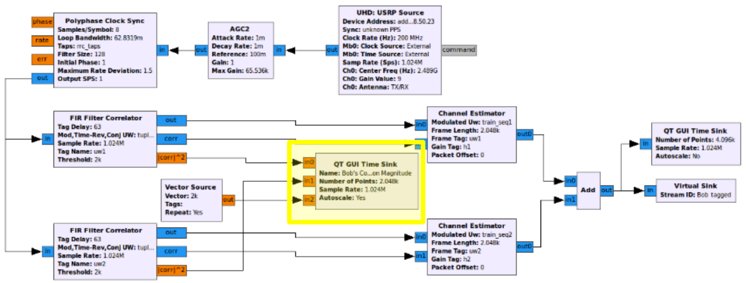
FIR FILTER CORRELATOR

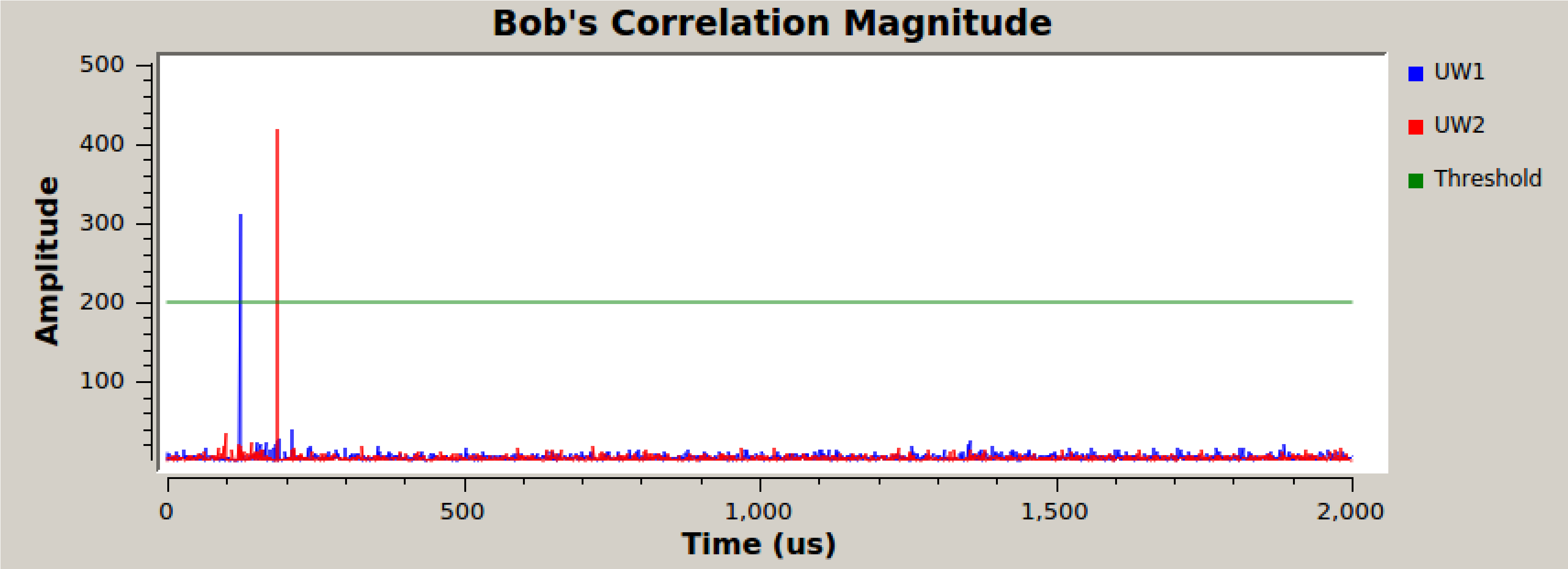


FIR FILTER CORRELATOR



EXAMPLE OUTPUT OF CORRELATOR





The output of the correlation filter can also be used to perform an estimate of the channel gains. Consider the cross-correlation of a unique word $w[n]$ of length N and amplitude 1 with the same unique word that experiences a complex Rayleigh flat fading gain h

$$R(hw[n], w[n]) = \sum_{m=0}^{N-1} hw[m]w^*[m-n].$$

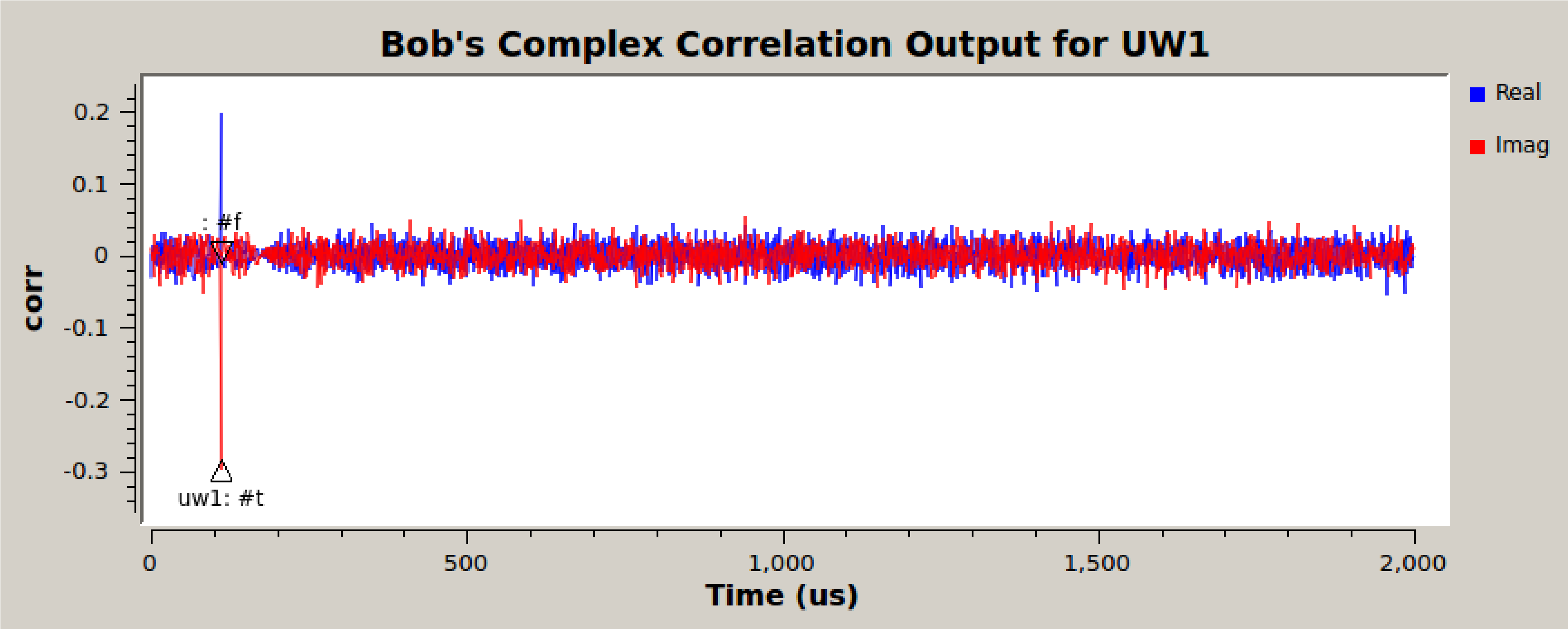
The peak value occurs when the unique words overlap at $n = 0$

$$R_{peak} = \sum_{m=0}^{N-1} hw[m]w^*[m] = Nh.$$

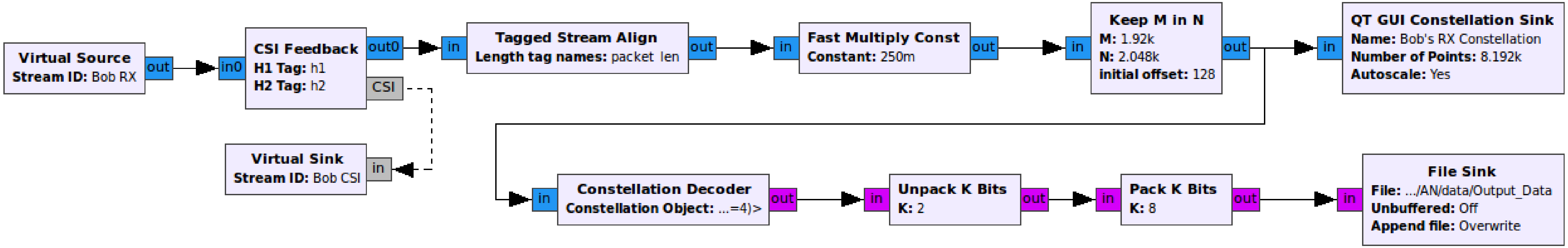
Therefore, the channel gain h can be estimated from the value of the correlation peak and the length of the unique word.

EXAMPLE OUTPUT OF CORRELATOR

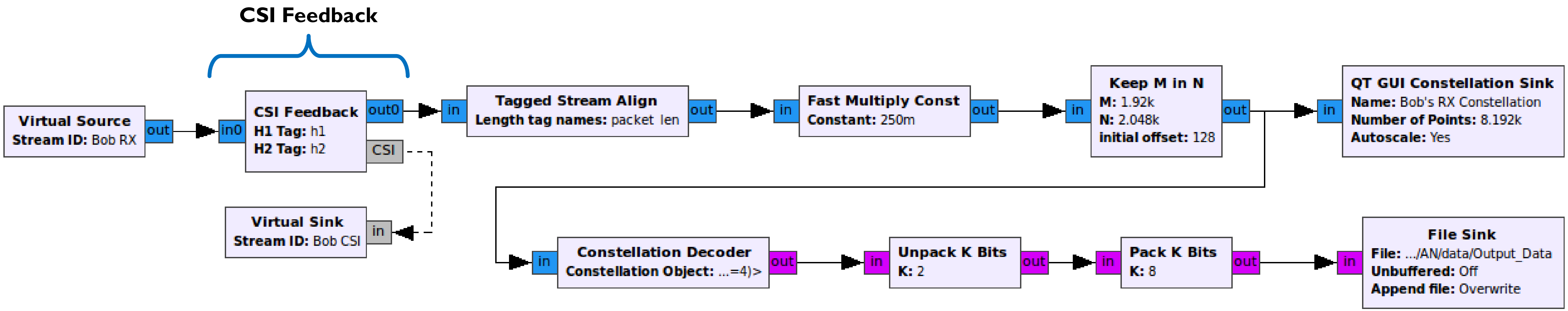
$$h = 0.20 - 0.30j$$



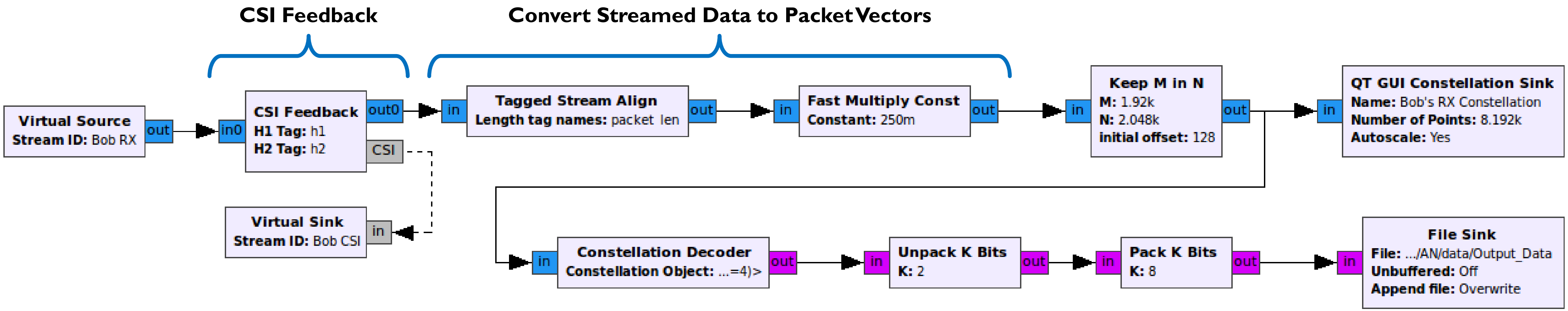
BOB'S ARTIFICIAL NOISE RECEIVER PART 2



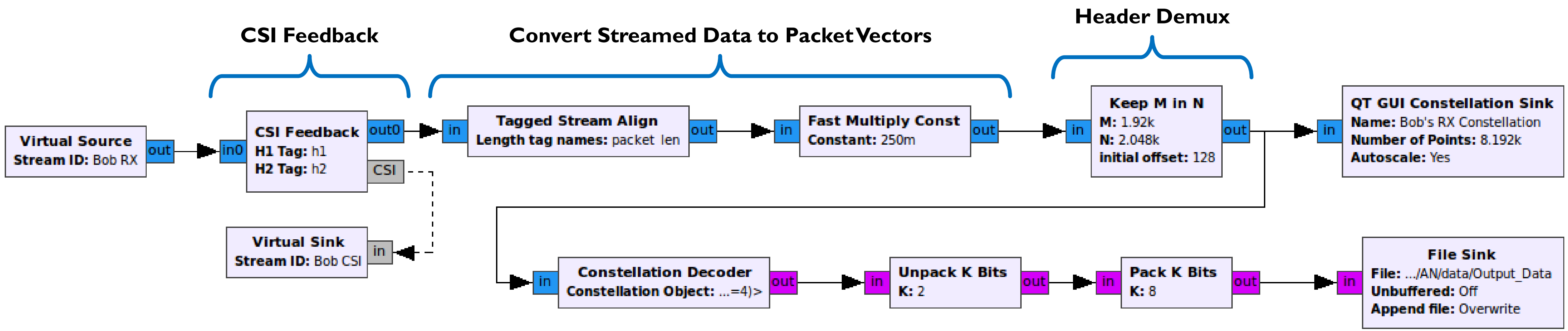
BOB'S ARTIFICIAL NOISE RECEIVER PART 2



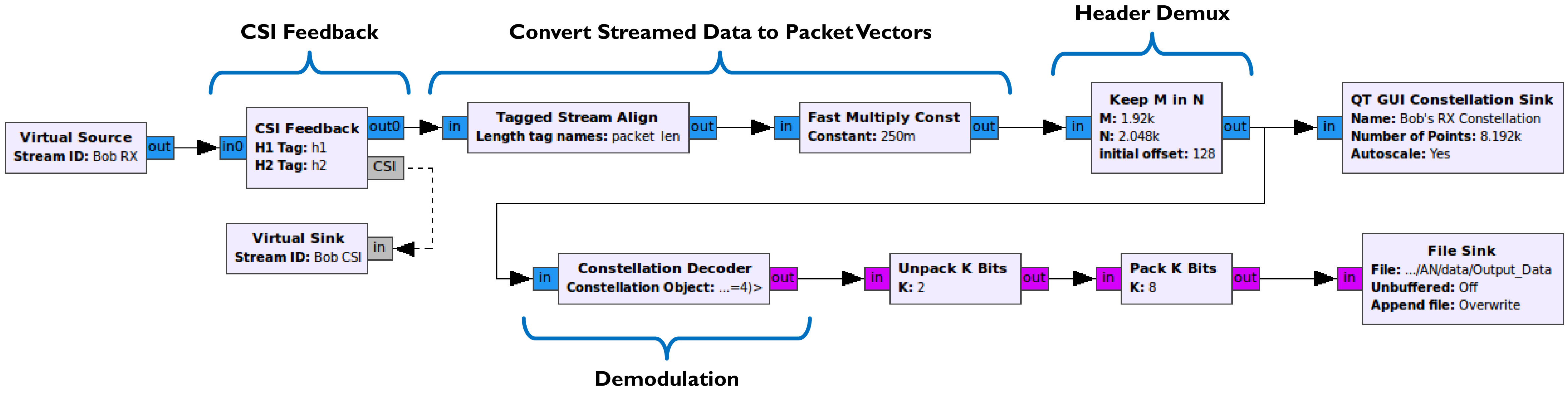
BOB'S ARTIFICIAL NOISE RECEIVER PART 2



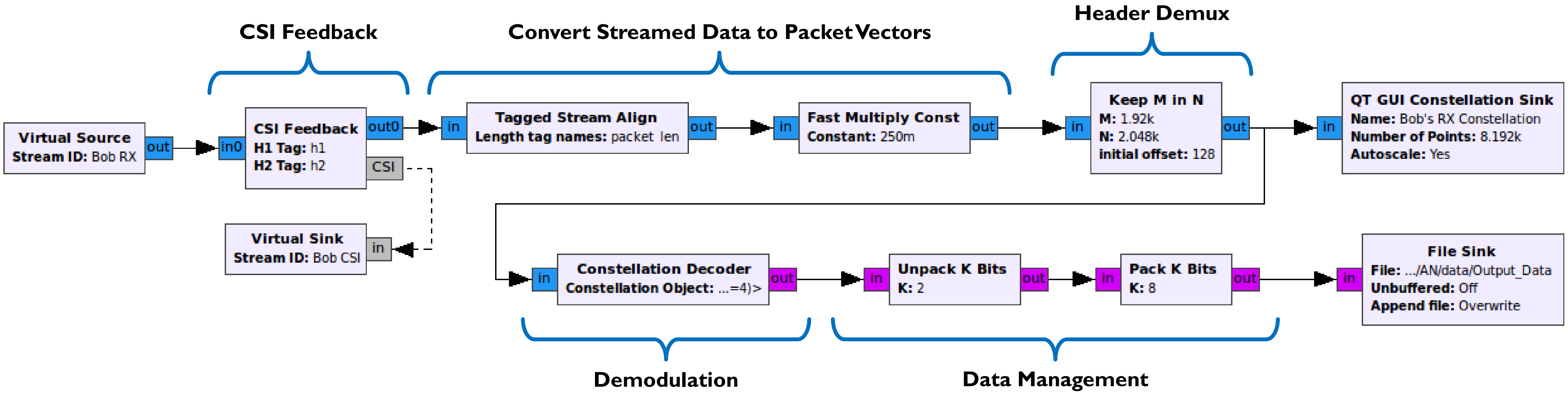
BOB'S ARTIFICIAL NOISE RECEIVER PART 2



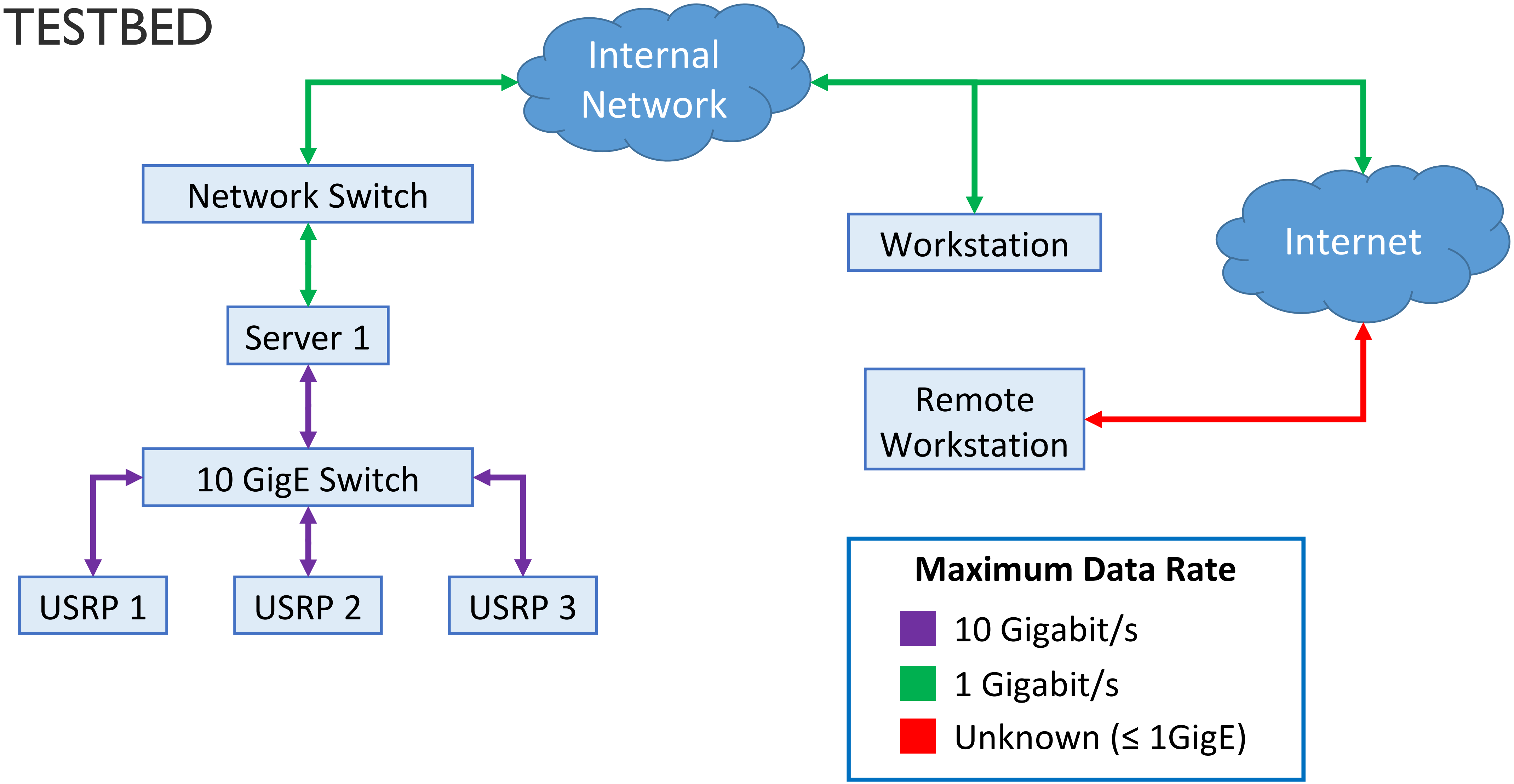
BOB'S ARTIFICIAL NOISE RECEIVER PART 2



BOB'S ARTIFICIAL NOISE RECEIVER PART 2

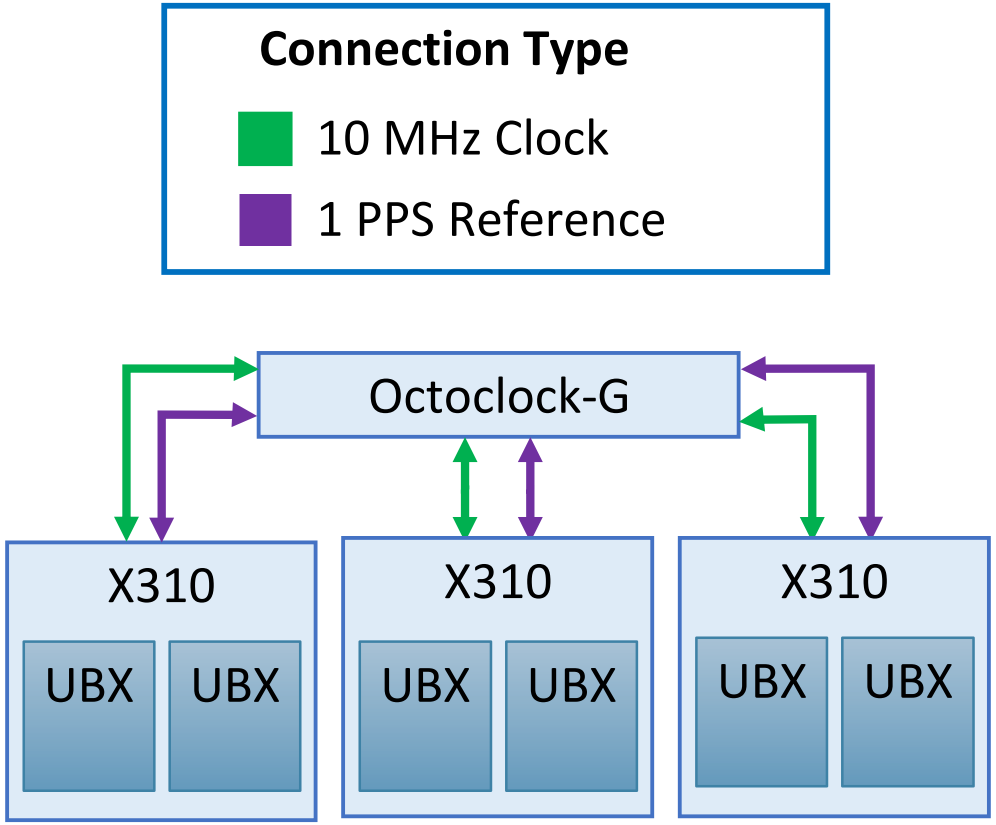


X310 TESTBED



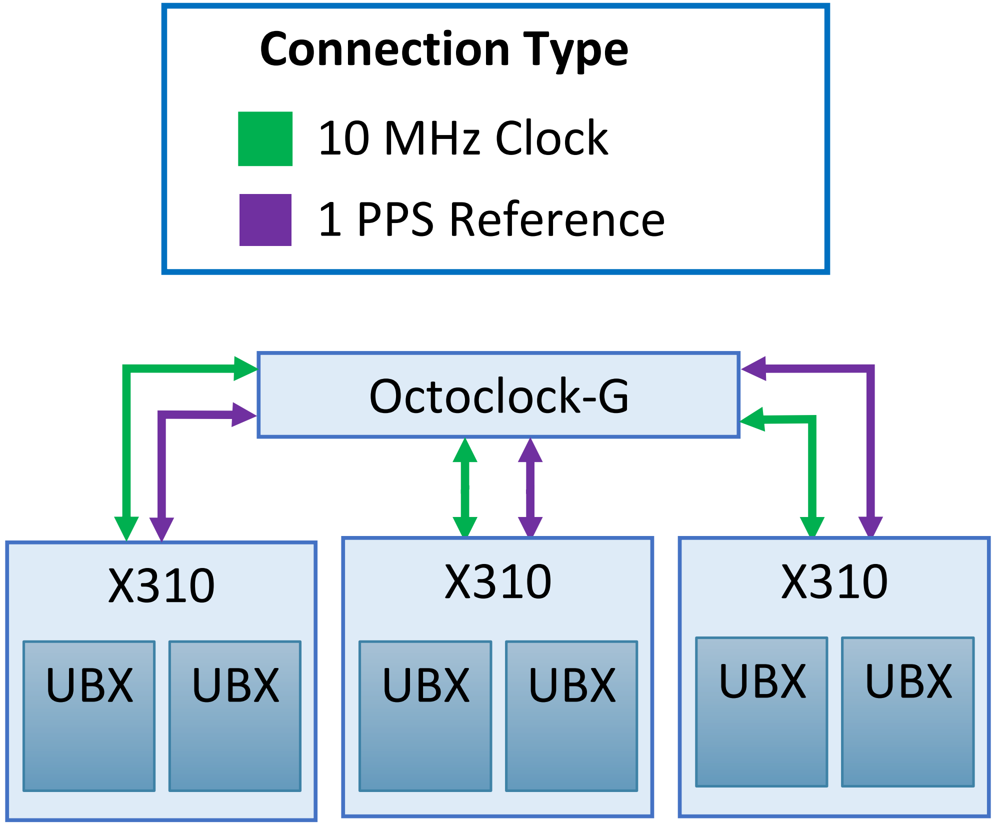
X310 TESTBED

Name	Quantity	Description
Ettus USRP X310	3	SDR Motherboard
Ettus UBX-160	6	SDR Daughtercard
Ettus Octoclock-G	1	Clock & Reference
Dell PowerEdge R820	1	Server
Intel SSD 3500 Series	4	800 GB SATA
Arista 7124SX	1	10 GigE Switch



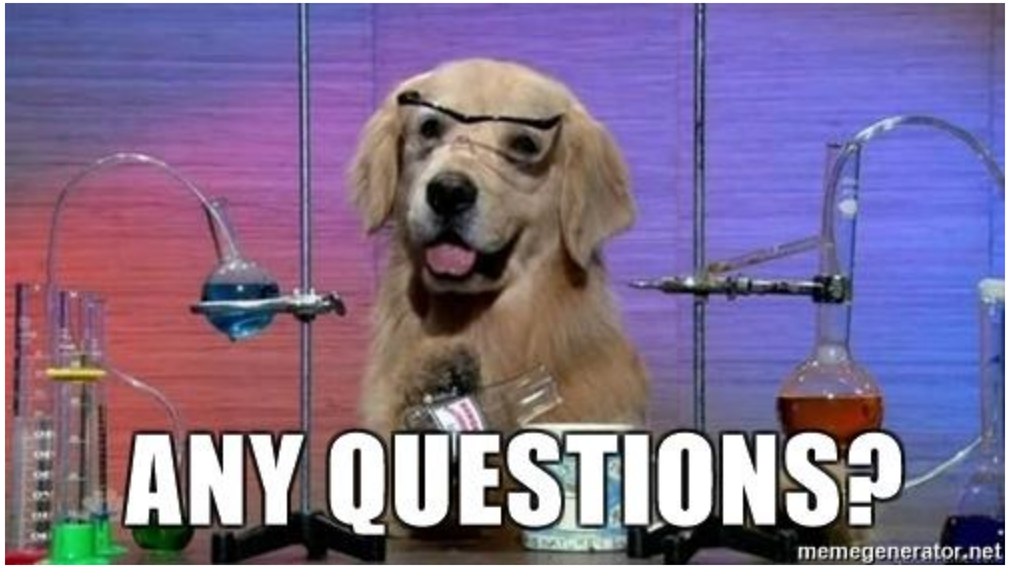
X310 TESTBED

Name	Quantity	Description
Ettus USRP X310	3	SDR Motherboard
Ettus UBX-160	6	SDR Daughtercard
Ettus Octoclock-G	1	Clock & Reference
Dell PowerEdge R820	1	Server
Intel SSD 3500 Series	4	800 GB SATA
Arista 7124SX	1	10 GigE Switch



DON'T FORGET THE DEMO

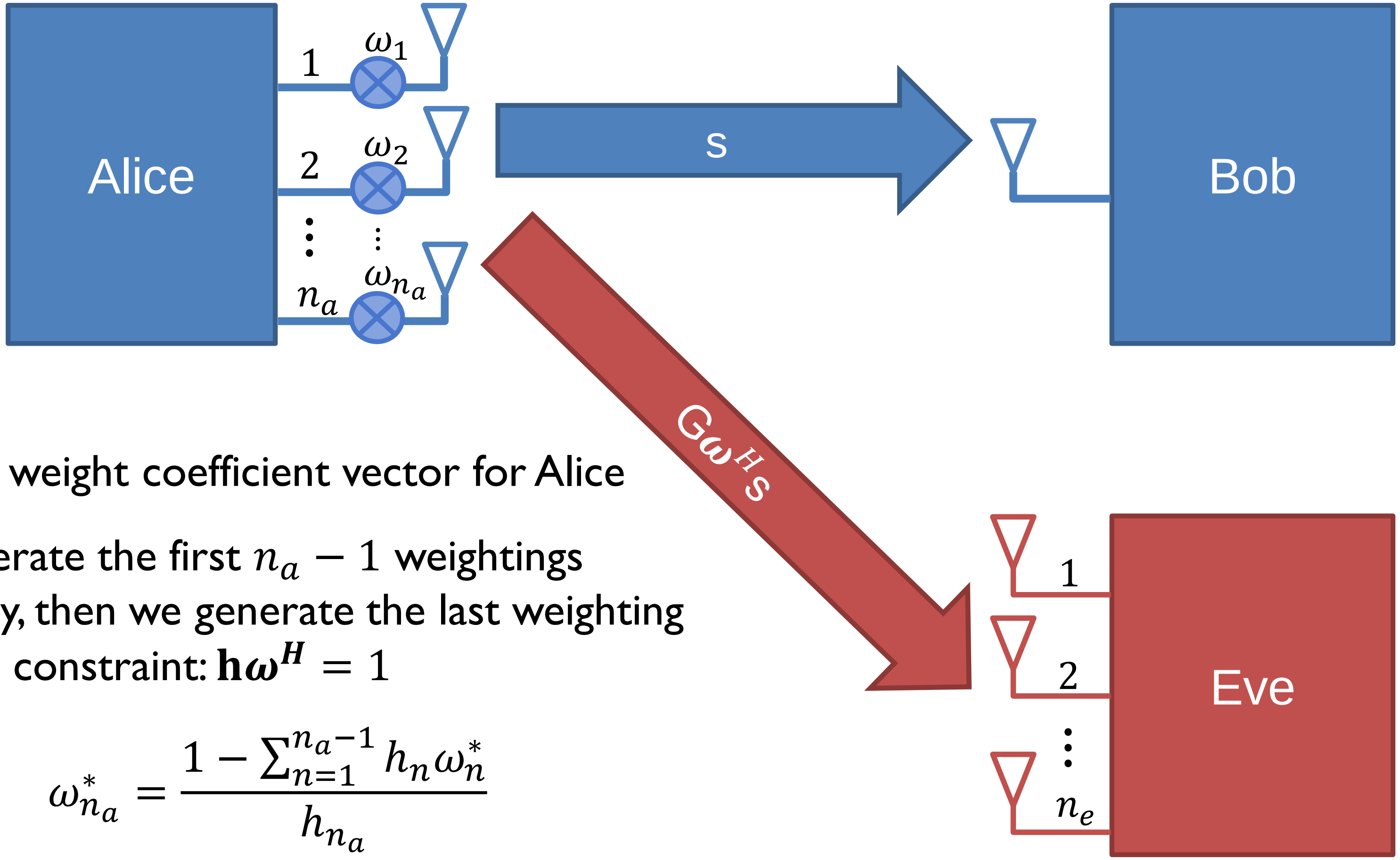
QUESTIONS?



OVERVIEW

- Intro to Physical Layer Security
- Background Information
- Artificial Noise Generation
- Phase-Enciphered Alamouti Coding
- Implementation
- Ongoing and Future Work

FUTURE WORK – ARTIFICIAL FAST FADING



Bob sees the source information and doesn't even need to undo the channel!

$\boldsymbol{\omega}$ is the weight coefficient vector for Alice

We generate the first $n_a - 1$ weightings randomly, then we generate the last weighting with the constraint: $\mathbf{h}\boldsymbol{\omega}^{\boldsymbol{H}} = 1$

$$\omega_{n_a}^* = \frac{1 - \sum_{n=1}^{n_a-1} h_n \omega_n^*}{h_{n_a}}$$

Eve sees a multiplicative distortion that's a function of $\boldsymbol{\omega}$ which we can vary with each transmitted symbol.

This results in fast fading at Eve, which prevents her from obtaining instantaneous CSI.