A Practical Method to Achieve Perfect Secrecy

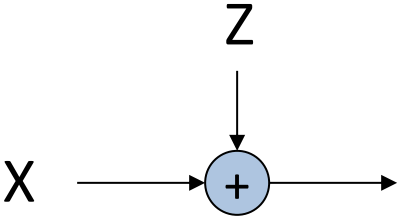
Amir K. Khandani

E&CE Department, University of Waterloo

August 3rd, 2014

Perfect Secrecy: One-time Pad

- One-time Pad: Bit-wise XOR of a (non-reusable) binary key with the message:

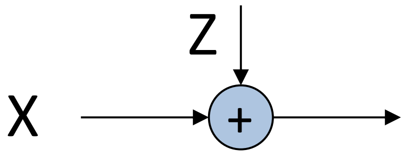


Y=X+Z (mod 2), X,Y,Z are binary, I(X;Y)=0

I(X;Y)=0 implies that the Eavesdropper (Eve) cannot extract any information about X (original data) by observing Y (encrypted data).

- A key of size N can encrypt a message with N-bits of data.
- Problems:
  - Content of the key should be communicated to both Alice and Bob, a procedure that is itself vulnerable to eavesdropping.
  - To guarantee perfect secrecy, each key should be used once, and never again.

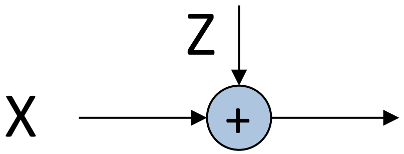
Generalization of XOR Encryption



$Y=X+Z \pmod{2\pi}$, X,Y,Z are angle, $I(X;Y)=0$

- Message X will be point of a PSK constellation, say a QPSK.
- Key Z is a random angle with uniform distribution in $[0,2\pi]$.
- $I(X;Y)=0$ means that the eavesdropper cannot extract any information about X (original PSK constellation point) by observing Y.

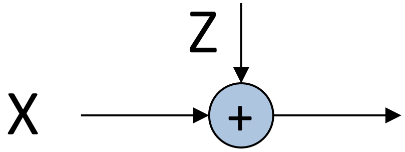
Generalization of XOR Encryption



Y=X+Z (mod 2π), X,Y,Z are angle, I(X;Y)=0

- **Key Points:**
  - Addition mod 2π occurs naturally in wireless propagation, where X is the phase of the transmitted constellation point and Z is the channel phase.
  - If Alice uses a 2^m-PSK modulation to send m bits to Bob, these m bits will be hidden from the Eve because the phase of the PSK constellation will be added with Z, where Z is the channel phase from the legitimate transmitter antenna to Eve's receive antenna.

Generalization of XOR Encryption



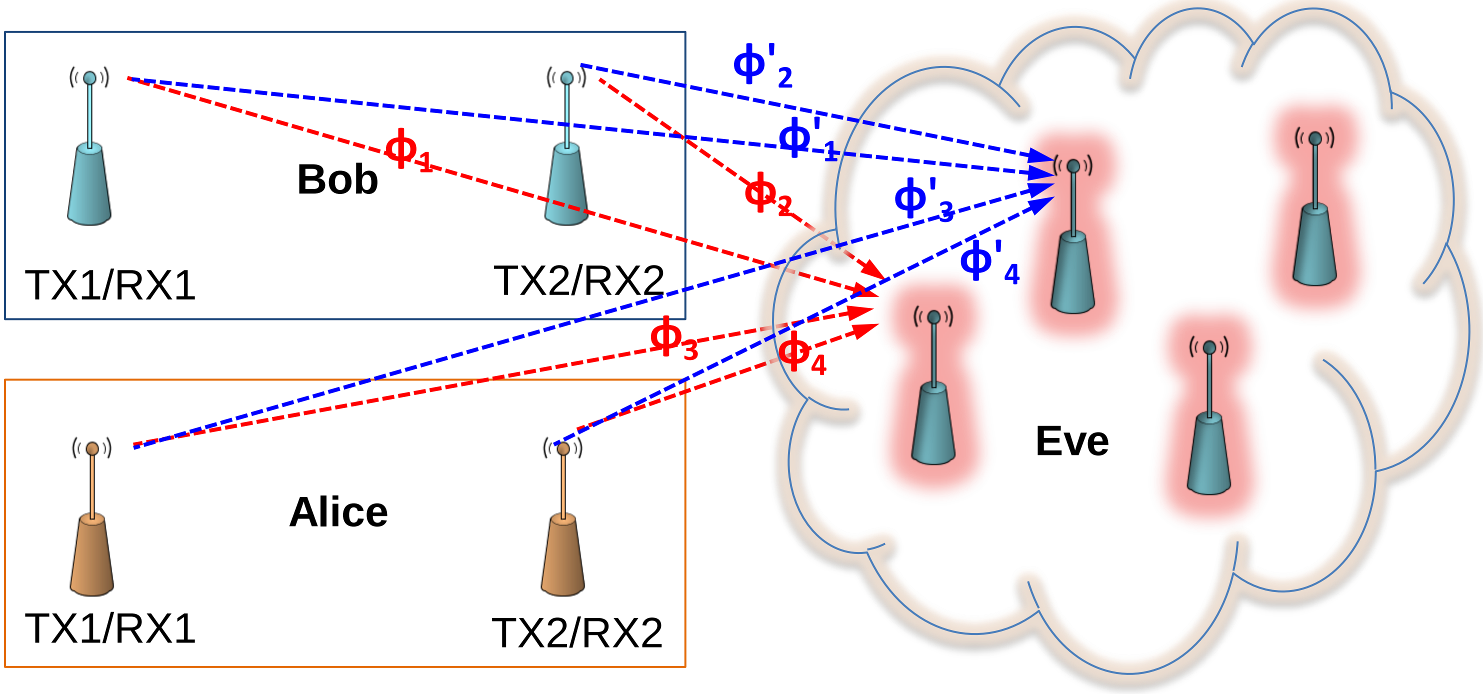
$Y=X+Z \pmod{2\pi}$, X,Y,Z are angle, $I(X;Y)=0$

- **Procedure:**
  - Alice and Bob get access to a set of, say n, shared random phase values known only to the two of them.
    - Shared phase values may have small errors from one party to the other one.
  - Alice (master) generates a set of n PSK constellation points with random data, rotate each of them with one of the shared phase values, and sends the rotated PSK constellation points to Bob (slave).
  - Bob, knowing the shared phase values, de-rotates the PSK constellations, and recovers its data.
  - Assuming a 2^m-PSK modulation and a FEC of rate r, after detection both units will have access to a secure key of size m x n x r bits.

Generating a Plurality of Shared Phase Values (i.i.d. uniform, Known to only Alice and Bob)

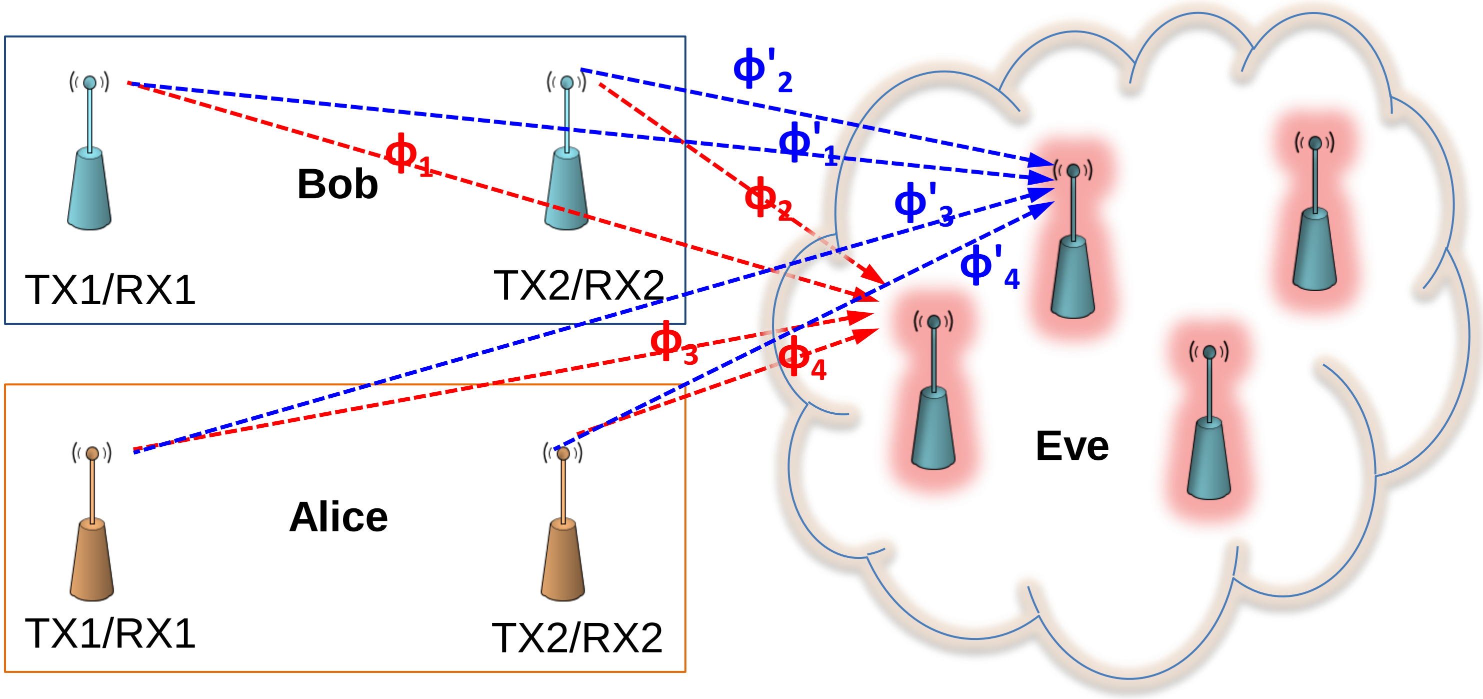
- **Key Points:**
  - Wireless channel is reciprocal in the sense that the phase of the channel from Alice to Bob is the same as the phase of the channel from Bob to Alice.
  - Phase of the channel can be changed randomly by perturbing the RF environment close to the Transmit (TX) antenna and/or close to the Receive (RX) antenna.
  - Variations caused by the RF perturbations close to the TX and/or RX antennas will be augmented by multi-path propagation of the RF signal as it travels from TX to RX.

How to Guarantee Perfect Secrecy?



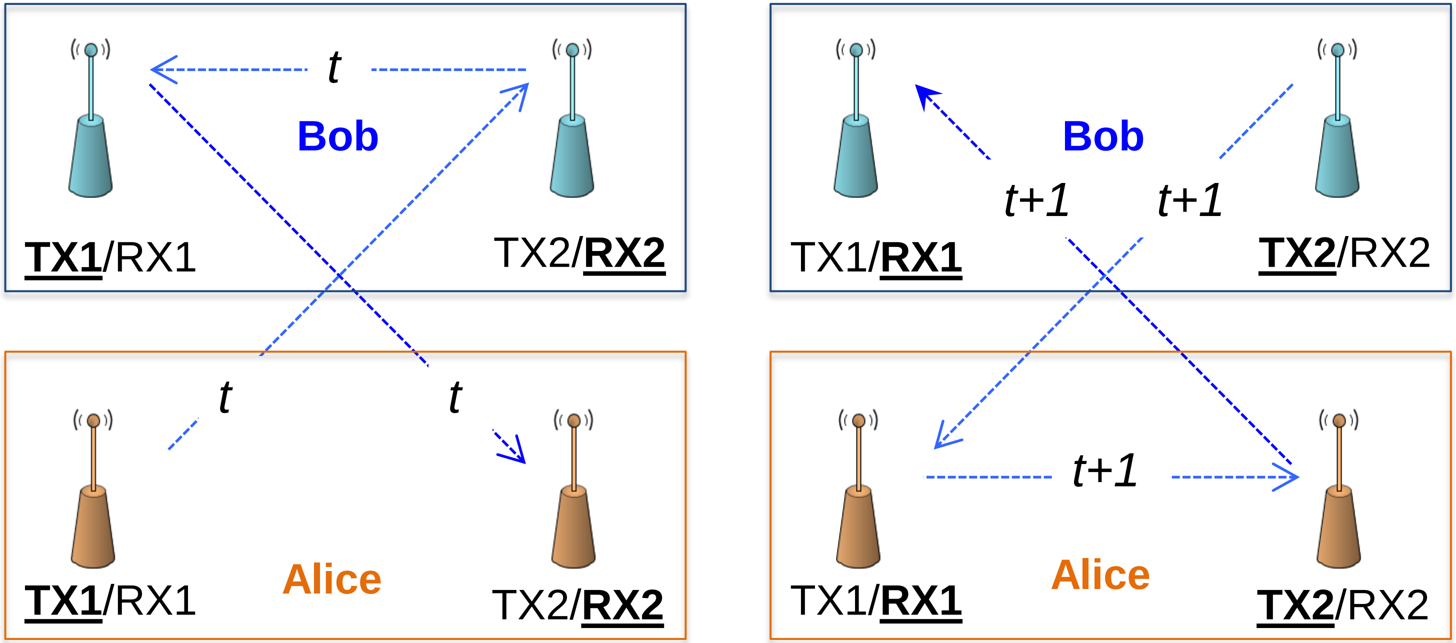
- There are four legitimate antennas, two in each legitimate node, and there will be four transmissions in total in each new channel state.
  - **Key point**: In each new channel state, there is a single transmission from each legitimate antenna, and then the channel state is changed. As a result, phases to all the Eve's antennas will change in every new channel state.

How to Guarantee Perfect Secrecy?



- **Key Point:**
  - Changing the channel state will change the channel phase to each of the Eve's receive antennas.
- Assume Eve has a large number of antennas with high SNR.
  - Each of Eve's antennas receives four signals, but each such signal is rotated with an unknown phase and conveys no useful information.

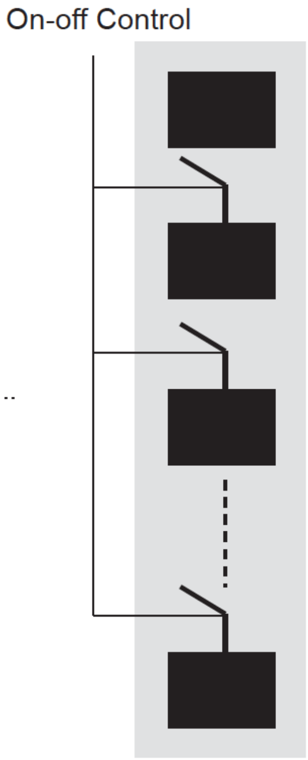
Generating a Plurality of shared Phase Values



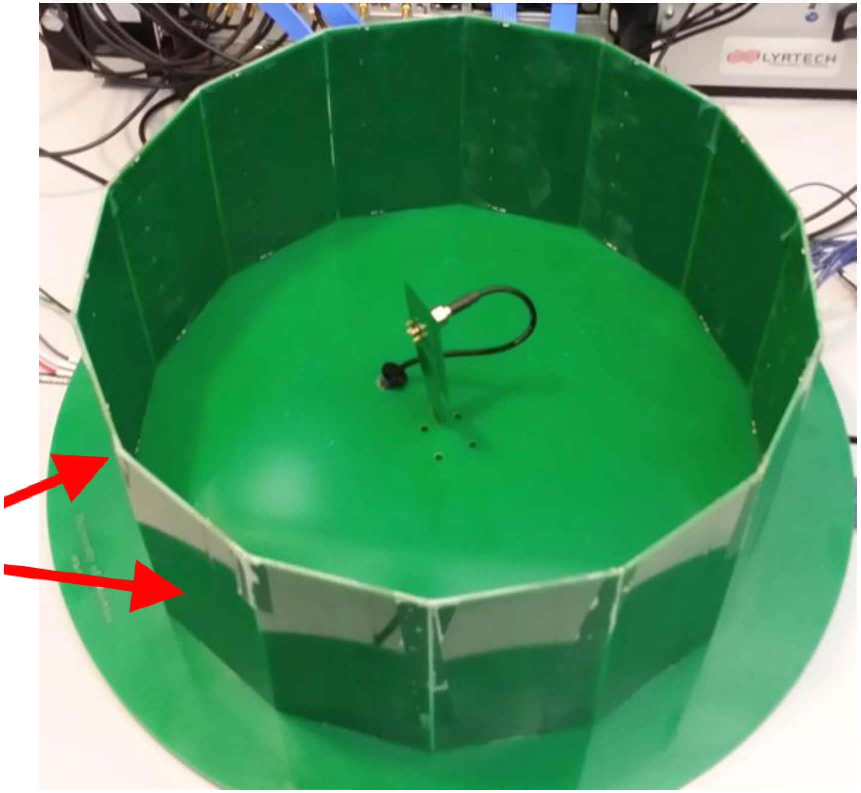
- At step *t*, Alice/TX1 (1st antenna of Alice acting as a TX antenna) sends pilots (to further enhance security, this pilot can be precoded with a random phase known only to Alice) to Bob/RX2 (2nd antenna of Bob acting at an RX antenna). Bob demodulates the received signal, and then re-modulates it and sends it using Bob/TX1 (1st antenna of Bob acting at a TX antenna) to Alice/RX2 (2nd antenna of Alice acting at an RX antenna) .
- At step *t+1*, Bob/TX2 sends pilots (to further enhance security, this pilot can be precoded with a random phase known only to Bob) to Alice/RX1. Alice demodulates the received signal, and then re-modulates it and sends it using Alice/TX2 to Bob/RX1.
- The two units, knowing their loop-back (internal) channels and relying on reciprocity, compute the following common phase values:
  - Alice: (Alice/TX1→Bob/RX2)x(Bob-loop-back)x(Bob/TX1→Alice/RX2)
  - Bob: (Bob/TX2→Alice/RX1)x(Alice-loop-back)x(Alice/TX2→Bob/RX1)
  - Then, RF environments **at the neighborhood of both Alice and Bob** are perturbed, and the procedure repeats to extract a new common phase value.

Actual Hardware
(case without exterior metallic strips)

There can be two antennas surrounded within a single RF closure at each node, or each (of the two antennas) can have its own RF closure (as shown below).



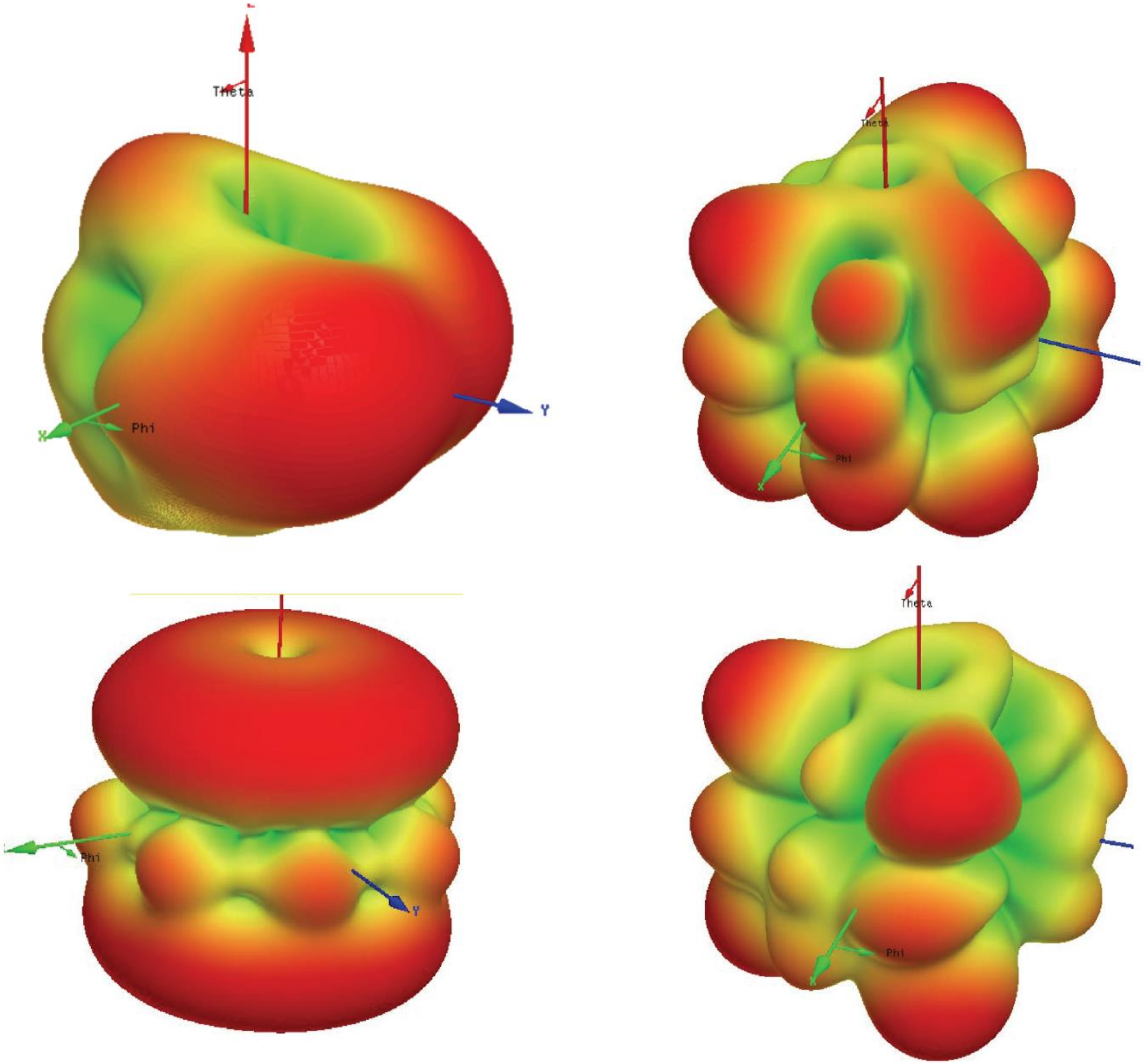
RF Mirror



14 RF Mirrors ➔ 2^{14} channel states for **each** RF closure.

Using four RF closures, one for each antenna, results in a total of 2^{56} combinations.

Examples of Antenna Patterns



Procedure for Generating a Key

Establishing the common phase values:

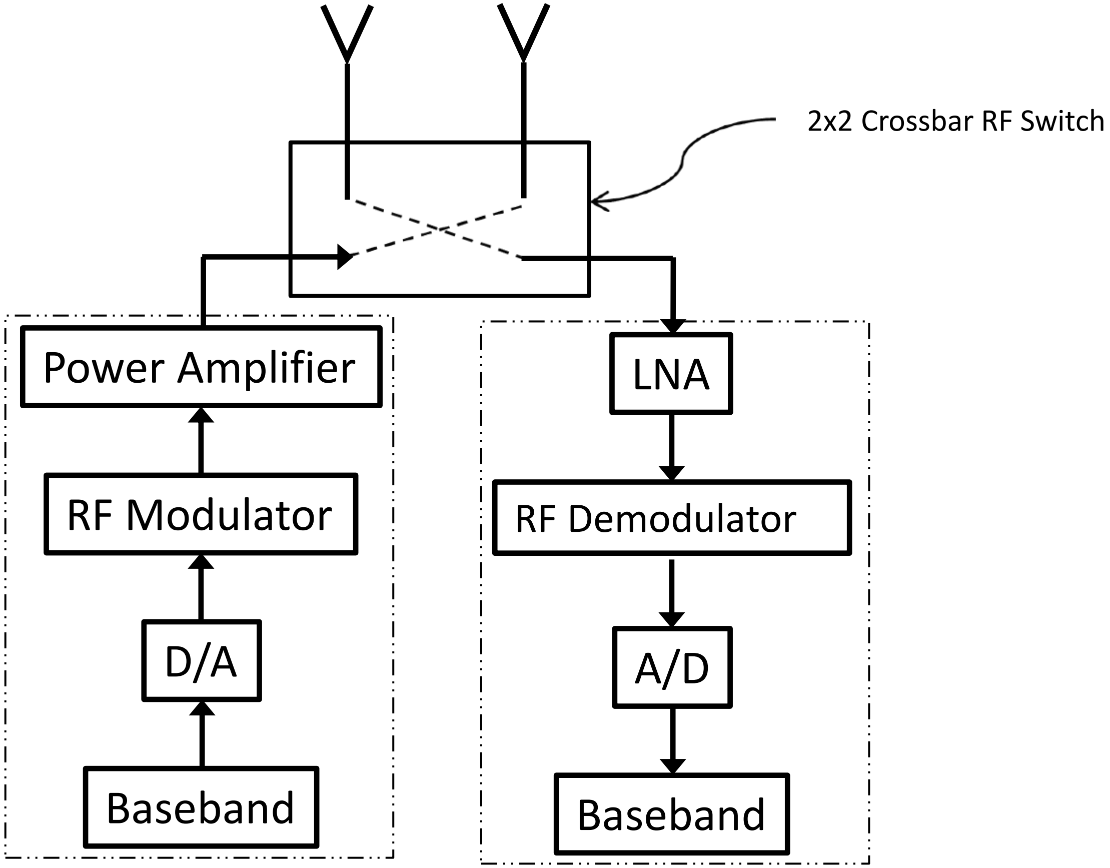
1. Perturb the channels at both Alice and Bob (switch all RF closures to a new random state by using a random On-OFF arrangement)
2. Establish a common phase value using the method explained earlier.
3. Go to step 1, and loop until enough common phase values, say n, are generated.

Generating the key:

1. Master generates a set of m x n x $(1\text{-}r)$ random bits (to become the final key), and encodes them using a FEC of rate r to obtain m x n coded bits.
2. Each m of such bits are mapped to a point in a 2^m points PSK constellation, and each PSK constellation is rotated by one of the common phase values.
3. n such rotated PSK constellation points are transmitted from the master to the slave.
4. Salve de-rotates the received constellation points by its local copy of the corresponding shared phase value, demodulates the de-rotated PSK constellations, and finally decodes the FEC to extract the random bits generated by the master.

Note that the rate of the FEC is adjusted to correct any initial phase discrepancies between the shared phase values, plus correcting errors due to channel noise.

Changing the Roles of TX and RX Antennas



Method to Perturb the RF Channel

- Alice and Bob each have two antennas where each of these two antennas can be used as TX antenna or as RX antenna, selectable through a 2x2 crossbar RF switch.
- Option 1:
  - At each unit, the two antennas are surrounded by a set of walls which act as ON/OFF RF mirrors (hereafter, called an RF closure).
  - Using K mirrors to build the RF closure at each node, one can obtain up to 2^{2K} channel states.
- Option 2:
  - Each antenna at each unit has its own RF closure, meaning there are a total of four RF closures, two at each node.
  - Using K mirrors to build each of the four RF closures (two at each node), one can obtain up to 2^{4K} channel states.

Privacy Amplification

- At the end, privacy amplification can be used to enhance the randomness in the final key.
- Privacy amplification is like multiplying a key of size P by a known binary random matrix of size QxP where P>>Q. This reduces the size of the key from P to Q, and thereby reduces the effect of any residual dependencies in the final key.

An Outstanding Concern

- We used the shared phase values to encrypt a random stream of bits to be used as the final key.
  - This was done to remove initial mismatches between the shared phase values (mismatches are due to measurement errors, noise and asymmetries in hardware).
- Does this one-time use of the key contradicts the requirement that the key cannot be reused?
- The answer is negative, as there is no redundancy in the encrypted message used in the first time application of the key (contains one bit of information per each binary digit).