Outline

- Concept:

Key distribution using electromagnetic reciprocity

- Capacity:

Bounds on key length, specifically the UWB case

- Communication:

Practical key exchange methods

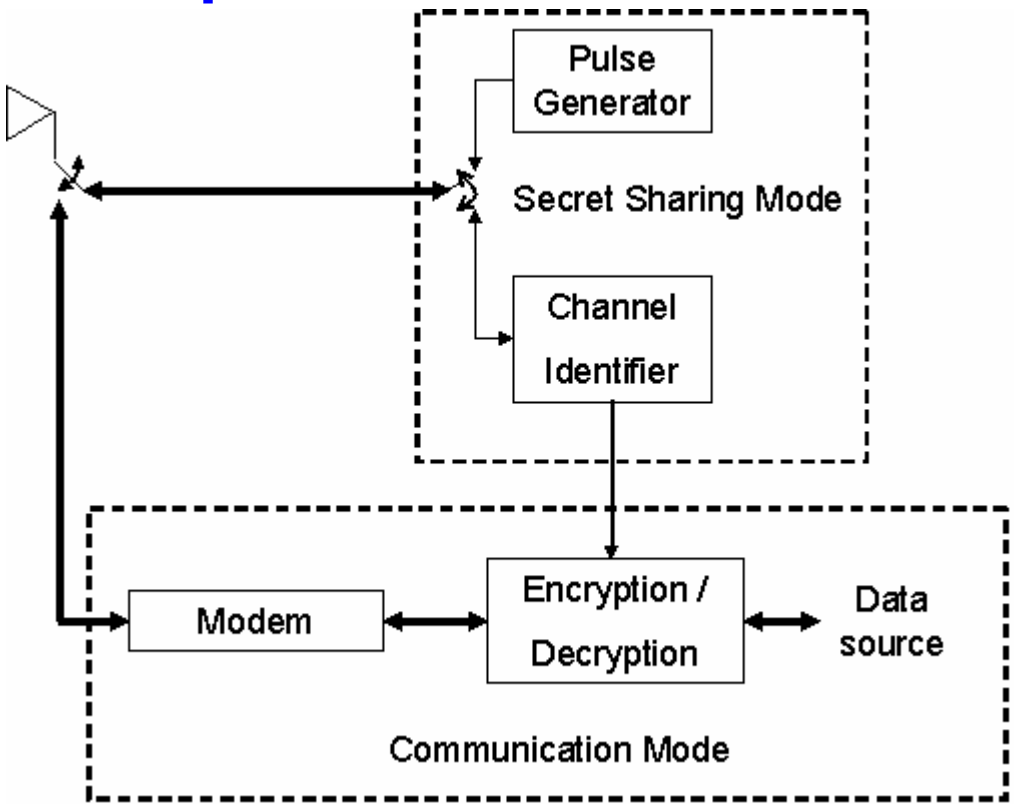
- Covertness:

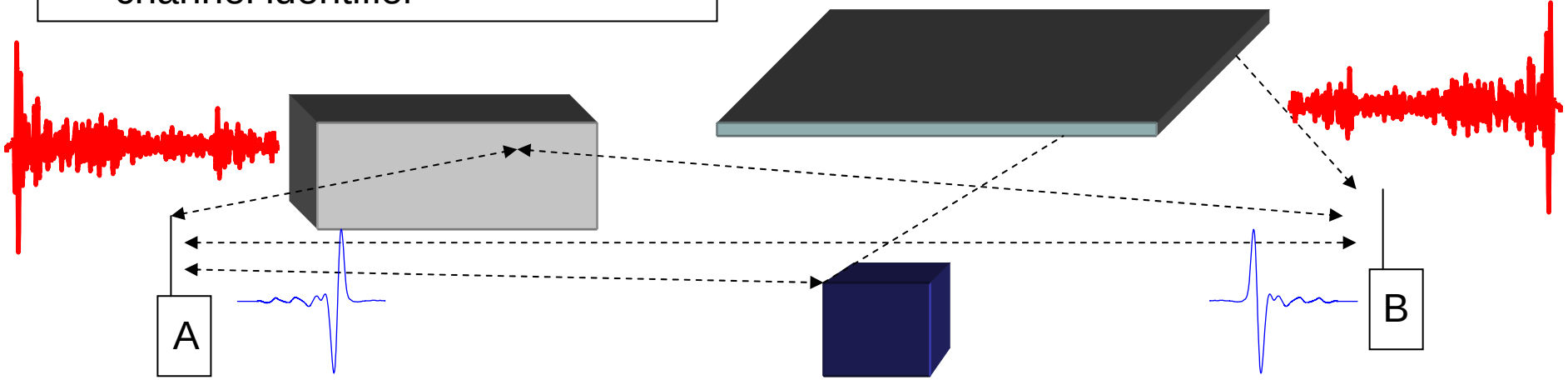
Immunity to eavesdropping

- Conclusions

Concept

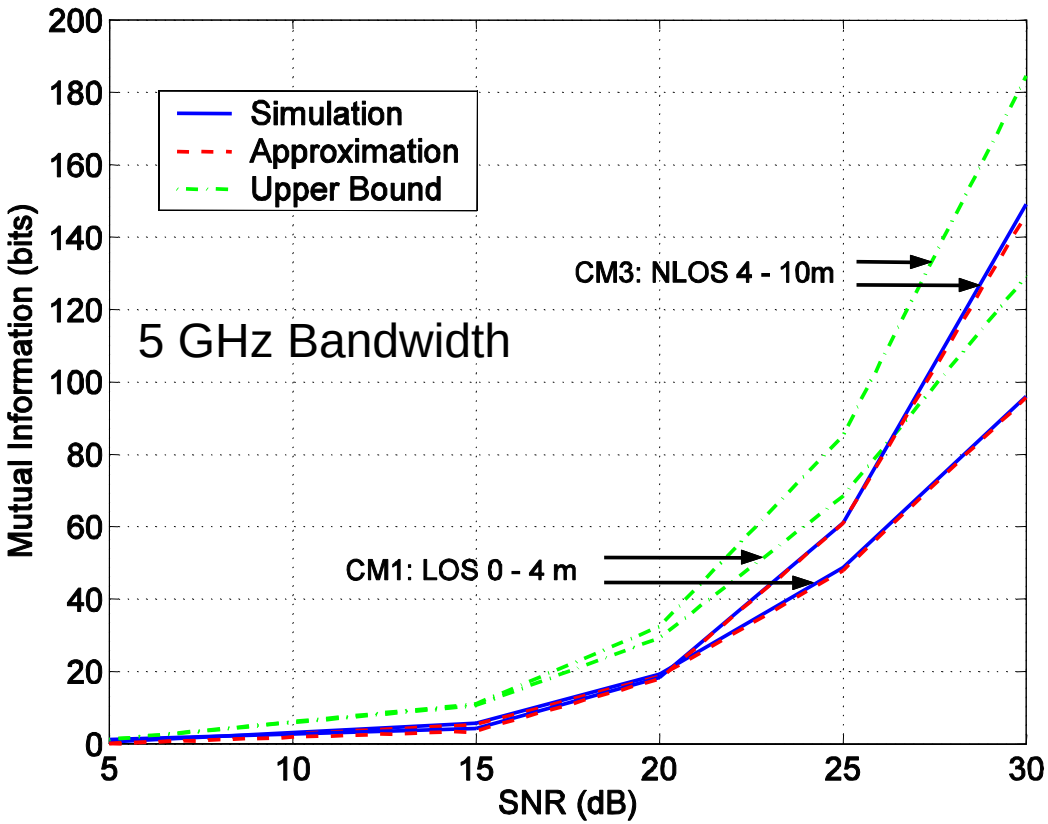
1. Each radio transmits an identical signal
2. Each radio observes the pulse response of the channel
3. The radios exchange some information about what they observed
4. Each radio calculates the channel identifier
5. The radios begin communicating data, encrypting it using the channel identifier





Capacity

- Secret communication capacity is determined by the randomness of the channel identifier
- Randomness is limited by the mutual information between the observations of Alice and Bob



Consider:

Signal power	-4dBm
Receiver NF	10dB
Channel loss exponent	3.75

30 dB SNR is equivalent to:

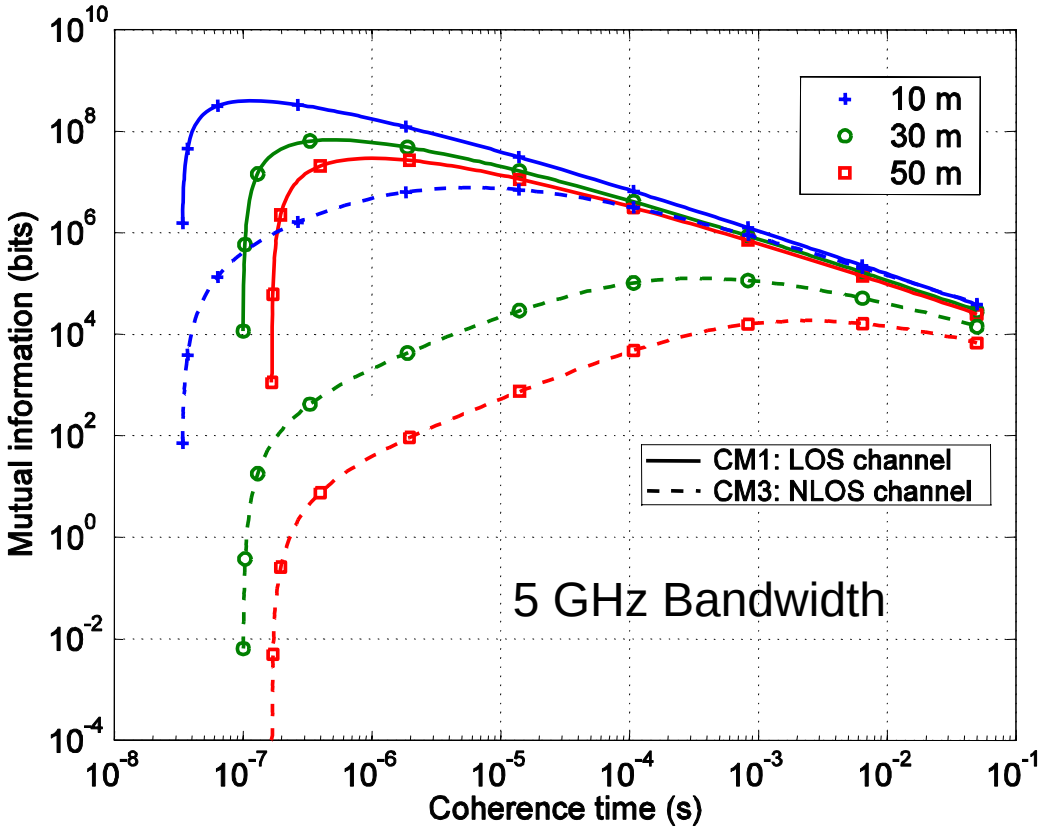
Tx-Rx distance	Integration time
3 m	270 ns
10 m	25 us
30 m	1.5 ms
50 m	10.5 ms

Capacity: mobility

- Achievable channel identifier length:

  – increases linearly with the number of independent channels observed, which increases linearly with speed of motion

  – increases logarithmically with the coherence time of each channel, which decreases linearly with speed of motion



- An optimal speed of motion exists for a given signal and environment

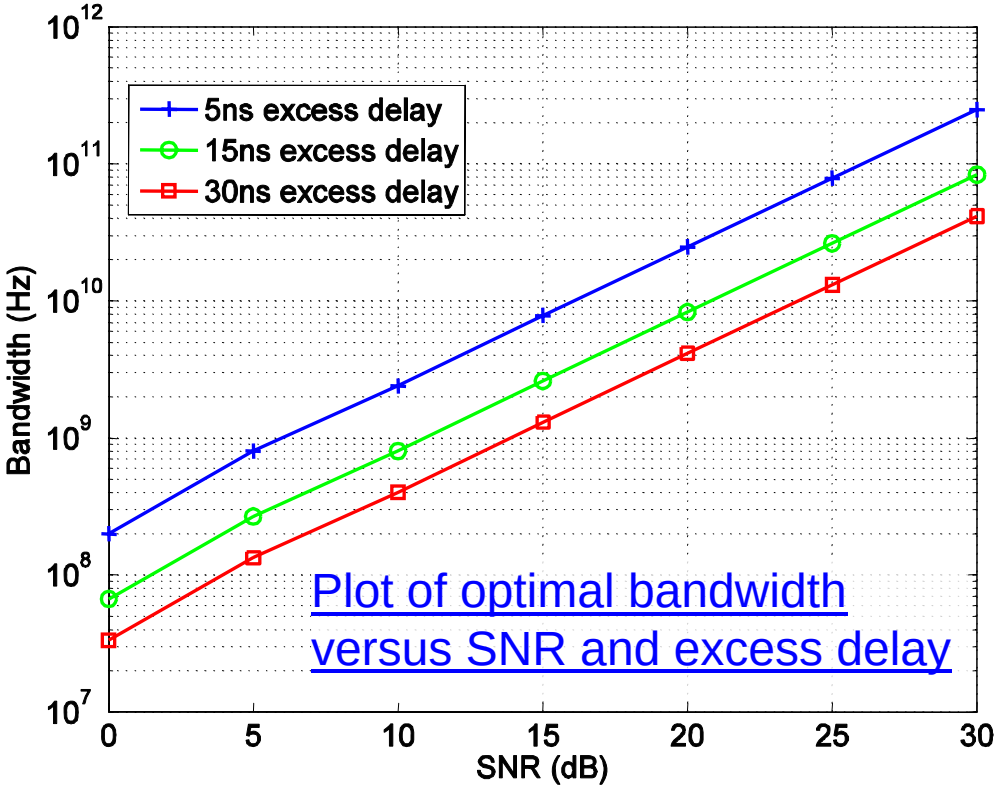
  – For a block fading model with independent, constant channels at 6-inch intervals, the coherence time at pedestrian speeds is > 22ms

  – With the curves shown on the left, this suggests faster is better in the pedestrian case

Capacity: bandwidth

• Mutual information doesn't increase monotonically with the number of channel taps, in fact:

$$I(X,Y) = \frac{L}{2}\log_2\left(1+\frac{E^2}{L.E\left(N_A+N_B\right)/2+L^2N_AN_B/4}\right) \xrightarrow{L\to\infty} 0\,!$$



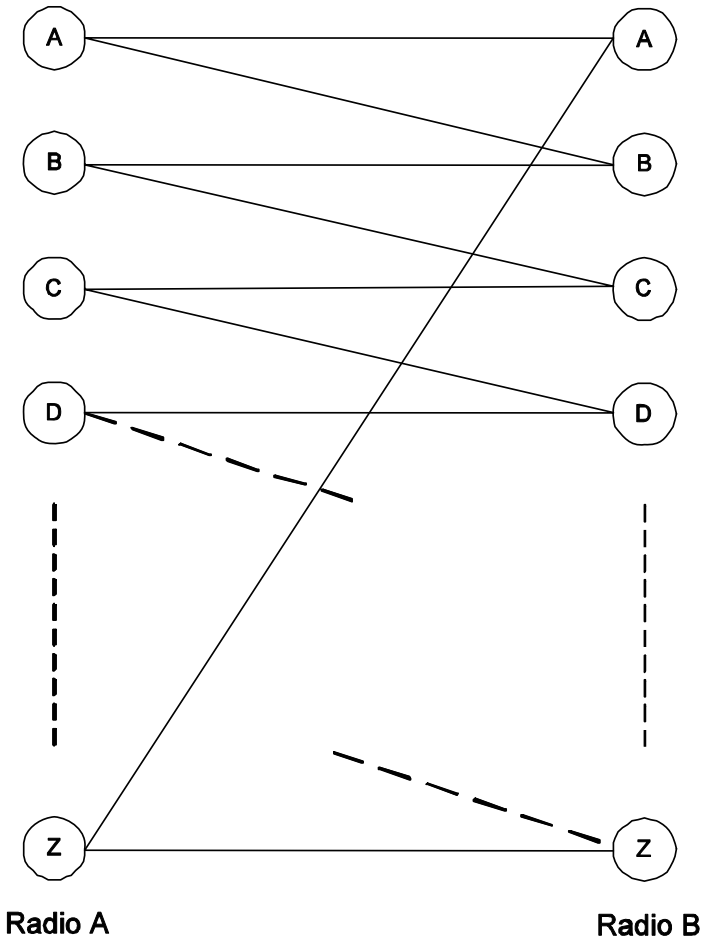
• When total SNR is fixed, the energy in each multipath component approaches zero as the number of components gets large

• The number of components is inversely proportional to bandwidth, thus an optimal bandwidth can be found

• The optimal bandwidth is in the UWB range in many cases

Communication

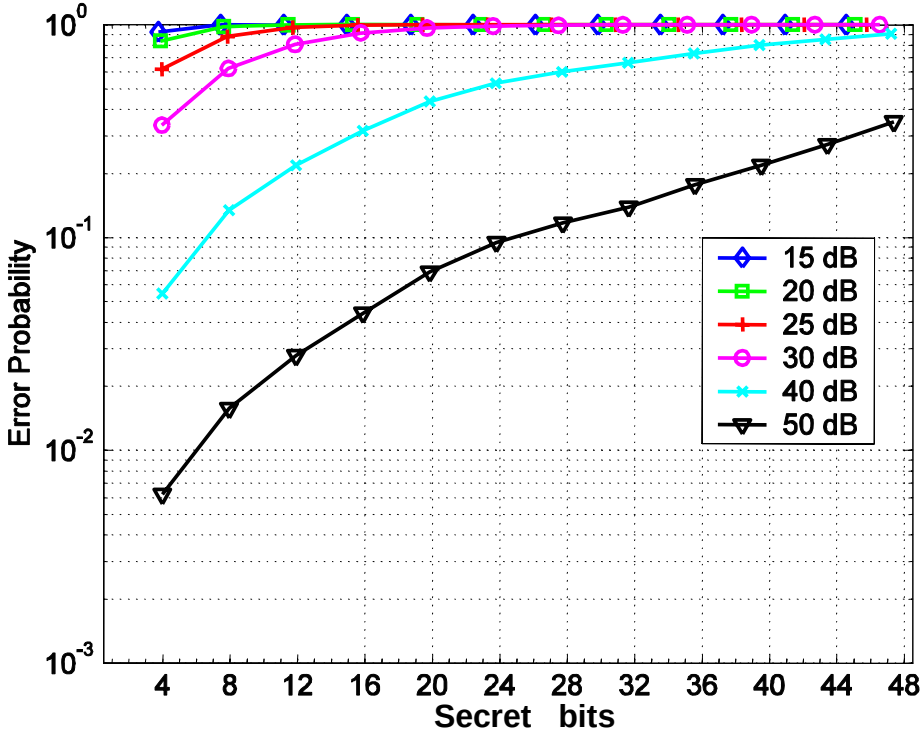
- The randomness of the channel identifier is I(X,Y) only with public discussion between Alice and Bob, otherwise it is zero.
- A simple example: the discrete noisy typewriter channel

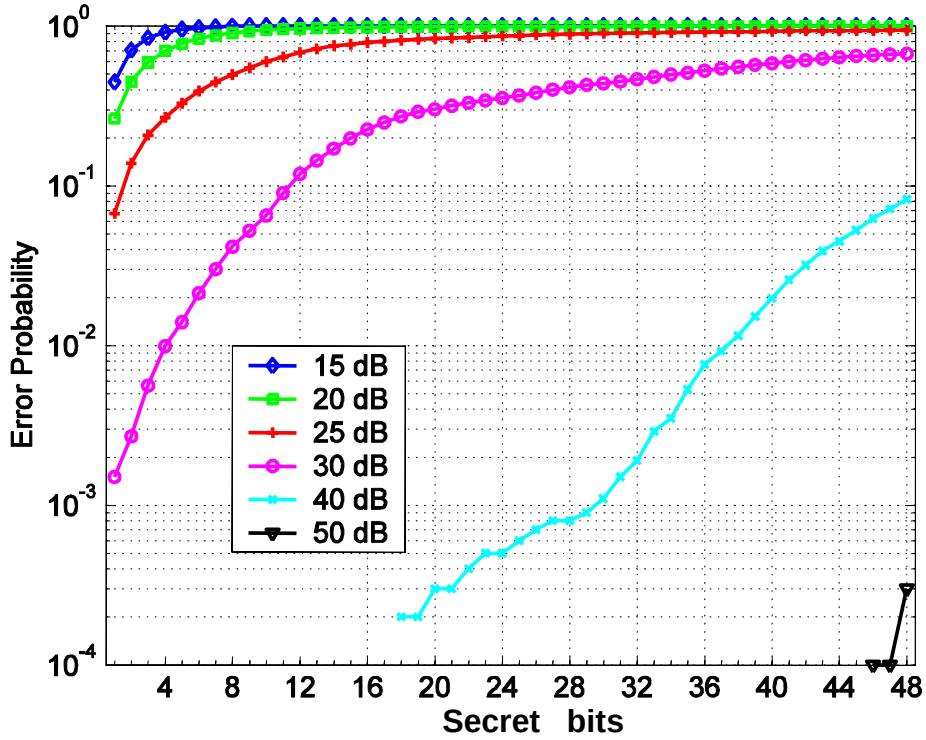


- Alice and Bob always make the same or adjacent observations
- To guarantee Alice and Bob get the same result all observations must map to a single identifier: no randomness = no secret communication capacity
- If Alice transmits one bit to Bob indicating which one of the two *cosets* {A,C,…,Y} or {B,D,…,Z} her observation lies in Bob can uniquely determine Alice's observation: identifier randomness = $\log_2(13)$
- Cosets can be defined over blocks or trellises to maximize the minimum distance between their members

Simulation Results

- Monte Carlo simulation over 10000 runs
- SNR is increased in practice by integrating over multiple pulses





- Reed-Muller coset assignment
- Single bit predictive quantization at each radio
- 1-bit of communication per secret bit

- Ungerboeck TCM coset assignment
- 3 bit predictive quantization at radio A, Viterbi soft decoding at radio B
- 5-bits of communication per secret bit

Experimental Results

- Channel measurements in opposite directions showed good agreement
- 3 bit quantization and trellis-based cosets were used with the real channel measurements to calculate channel identifiers
- An simulated eavesdropper (Eve) uses its own observation and the overheard public communication between Alice and Bob to guess their channel identifier

Number of bits before first error between Alice and Bob

Timing Error	0		50ps		500ps		1ns	
Feedback bits	1	2	1	2	1	2	1	2
Channel A	54	33	54	33	0	32	0	1
Channel B	2	32	6	32	4	17	0	4
Channel C	4	11	4	11	0	1	0	1
Channel D	4	4	4	4	0	2	0	1
Channel E	6	4	8	4	2	1	0	2

- Ideally, an eavesdropping receiver can correctly guess 50% of the identifier, but does not know which bits are correct

Percentage of identifier guessed by Eve

Feedback bits	1	2
Channel A	56%	63%
Channel B	59%	53%

Conclusions

- The channel impulse response can be used as a source of common information for secret key distribution
- The upper bound on identifier length is the mutual information between each radio's observation
- The mutual information over typical UWB channels is large enough for practical application
- The achievable identifier length is sometimes larger for mobile terminals than stationary ones
  - Under typical UWB conditions, and for a simplified fading model, achievable identifier length typically increases with speeds in the pedestrian range
- Achievable identifier length doesn't increase monotonically with bandwidth, and the optimal bandwidths are in the UWB range for typical indoor channel delay spreads
- Simulations demonstrated practical schemes for key distribution
- Initial simulations suggest good immunity to passive attacks