# Secret Sharing using Reciprocity in UWB Channels

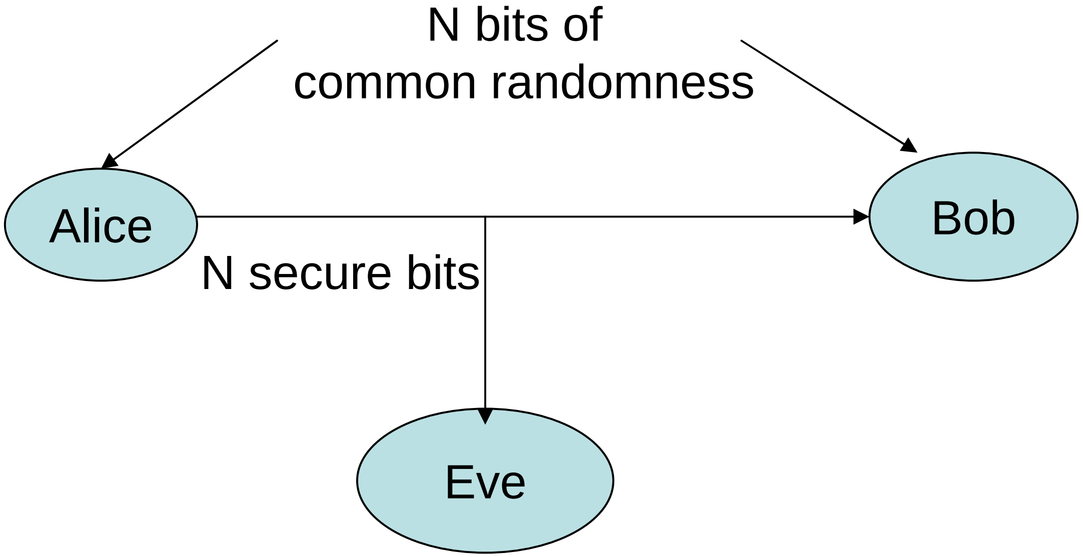
David Tse

U.C. Berkeley

Joint work with Robert Wilson and Bob Scholtz.

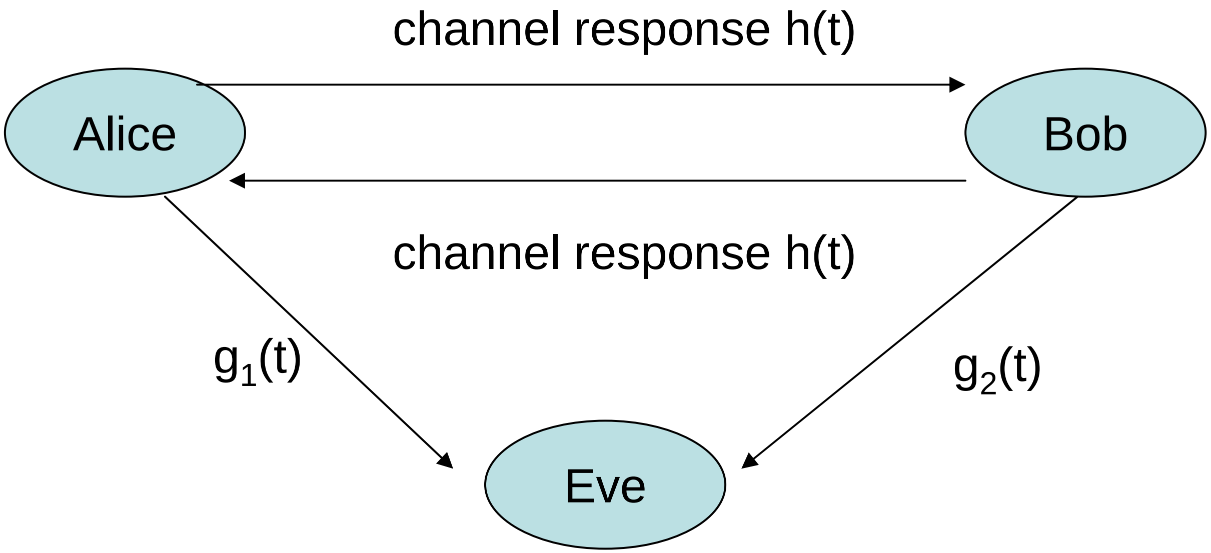
See Rob’s poster for more details.

# Secure Communication



- Shannon (1949) says: N secure bits needs N bits of common randomness (key) secret from Eve.
- Where on earth would these bits come from?

# Common Randomness via Reciprocity



- As long as Eve is not very close to Alice or Bob, $g_1(t)$ and $g_2(t)$ are more or less independent of h(t).
- h(t) provides common randomness secret from Eve.
- An UWB channel can potentially provide a lots of bits.

# Key Extraction from Reciprocity

- Alice sends an impulse to Bob, Bob observes

$$y_B(t) = h(t) + w_B(t)$$

- Bob does the same, Alice observes:

$$y_A(t) = h(t) + w_A(t)$$

- Problem: because of the independent noises at the receivers, Alice and Bob cannot agree on a secret key with high reliability.

# Reliable Secret Sharing

- Alice knows $y_A$, Bob knows $y_B$, correlated.

Theorem (Maurer 93):

Alice and Bob can share reliably a secret key of

$I(y_A;y_B)$ bits

…….provided that public discussion between Alice and Bob is allowed.

- Note: Eve can observe all the public discussion, but still knows nothing about the key at the end of the day!

# How can this be done?

- Example: Let $y_A$ and $y_B$ be random length-3 binary vectors, with correlation: Hamming distance between $y_A$ and $y_B$ is at most 1
  e.g. If $y_A=[0\ 1\ 0]$, $y_B$ can be $[0\ 1\ 0]$, $[0\ 1\ 1]$, $[0\ 0\ 0]$, or $[1\ 1\ 0]$

- Without public discussion, Alice and Bob cannot generate any common key reliably.

- Note: $I(y_A;y_B) = H(y_B)-H(y_B|y_A) = 3-2 = 1$

# Public Discussion via FEC

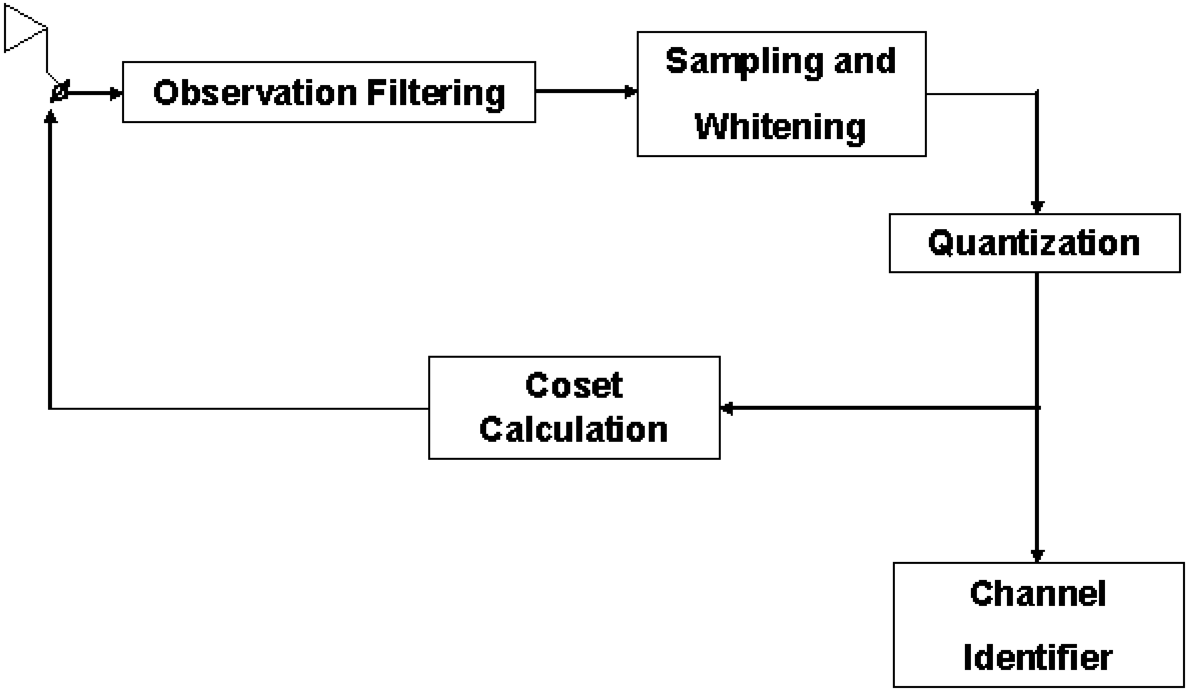
- Look at cosets of a length-3 repetition code:

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

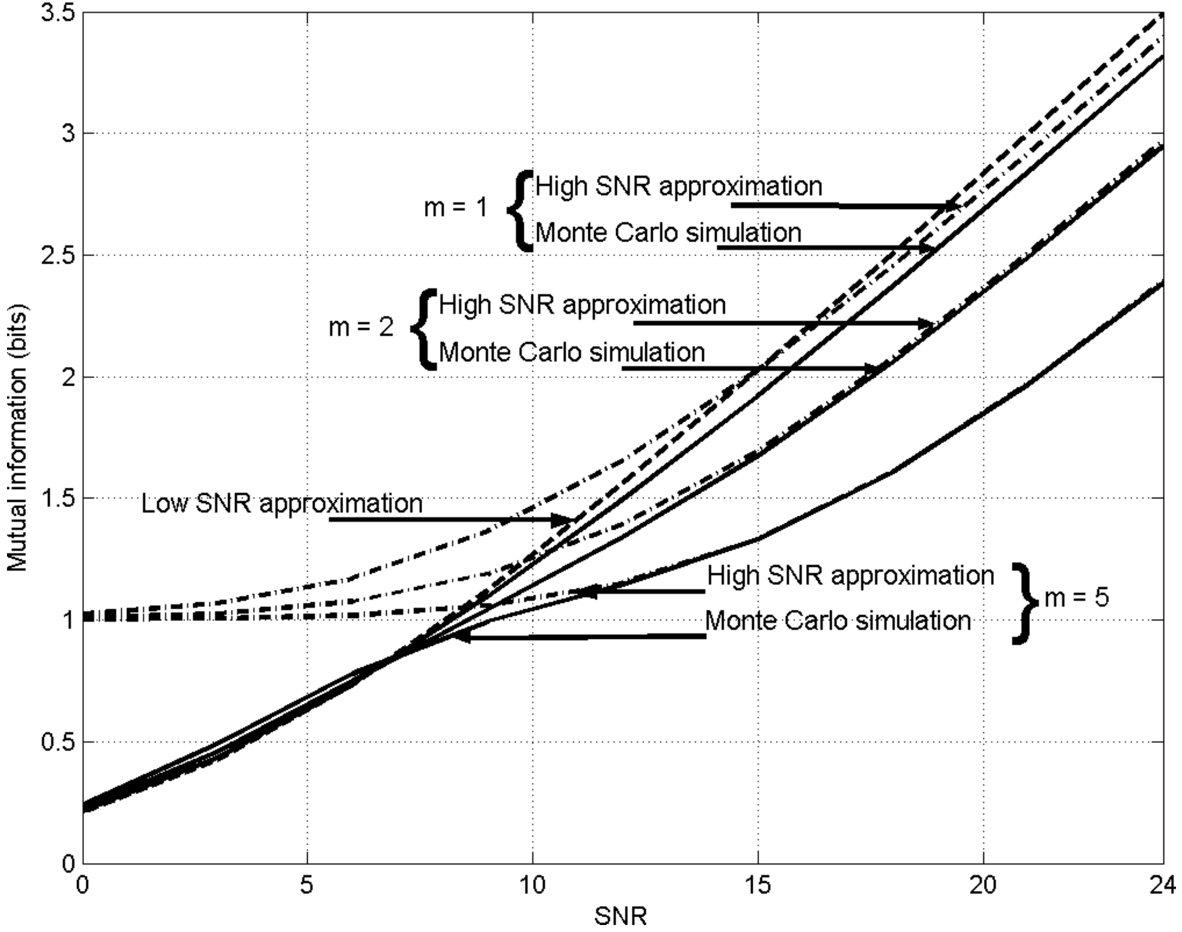
Coset-1 Coset-2 Coset-3 Coset- 4

- Alice sends the index of the coset containing $y_A$.
- Using index and $y_B$, Bob reconstructs $y_{A.}$
- The index of $y_A$ within its coset can serve as the shared key (1 bit in this eg.).
- Eve observes the coset index, but has no idea of the shared key.

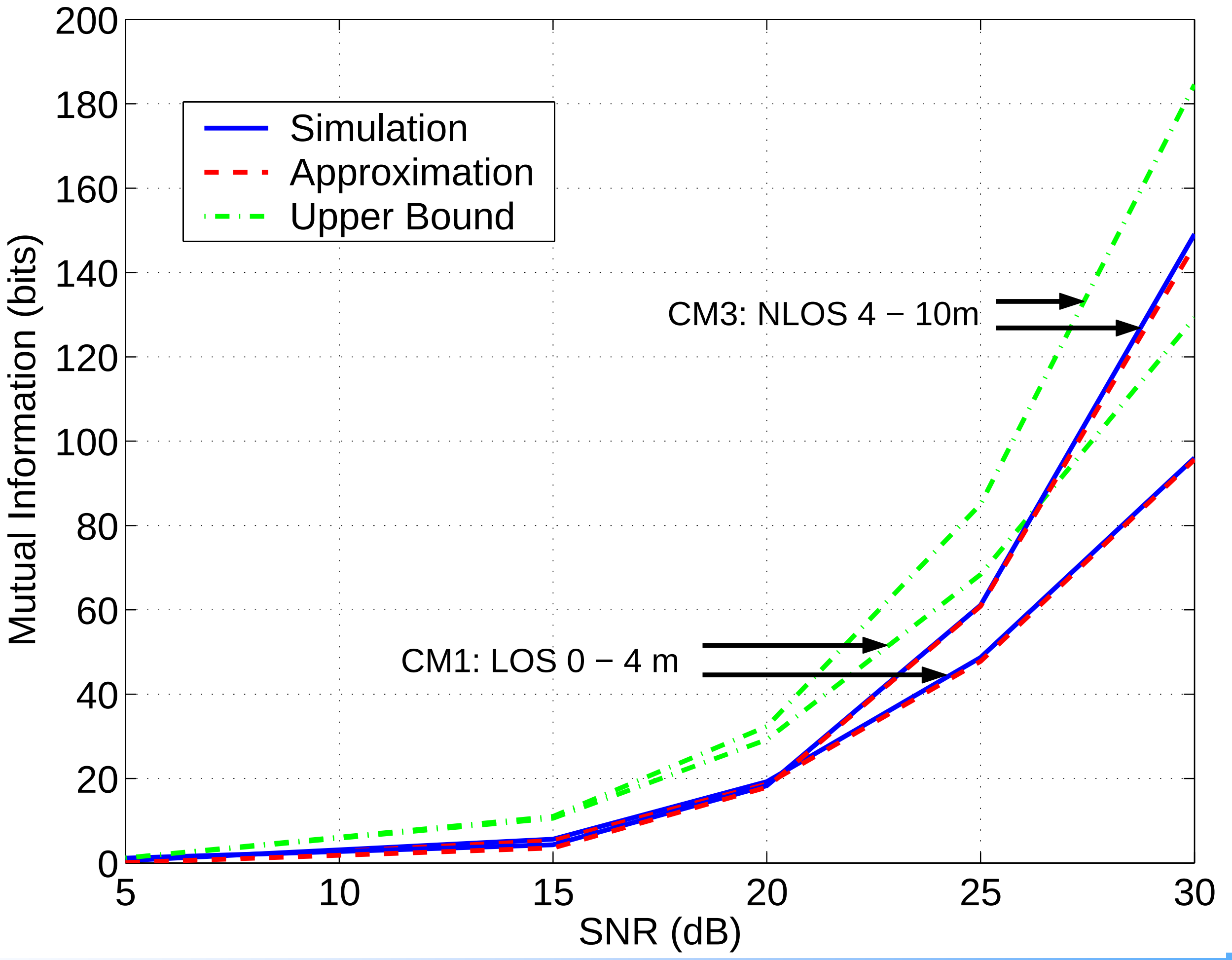
# Key Extraction System



# Mutual Information for Single Path Channel

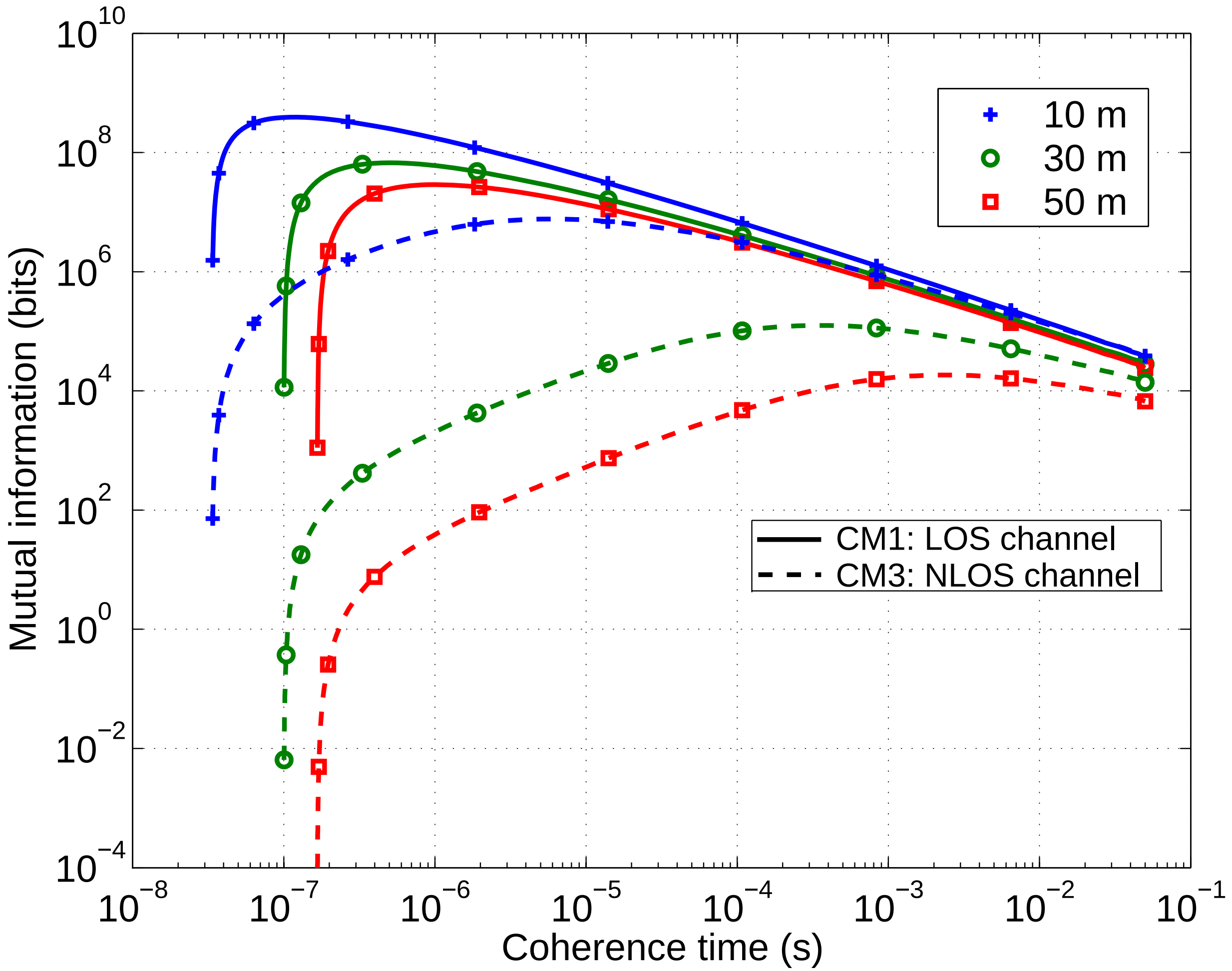


# Multipath UWB Channels

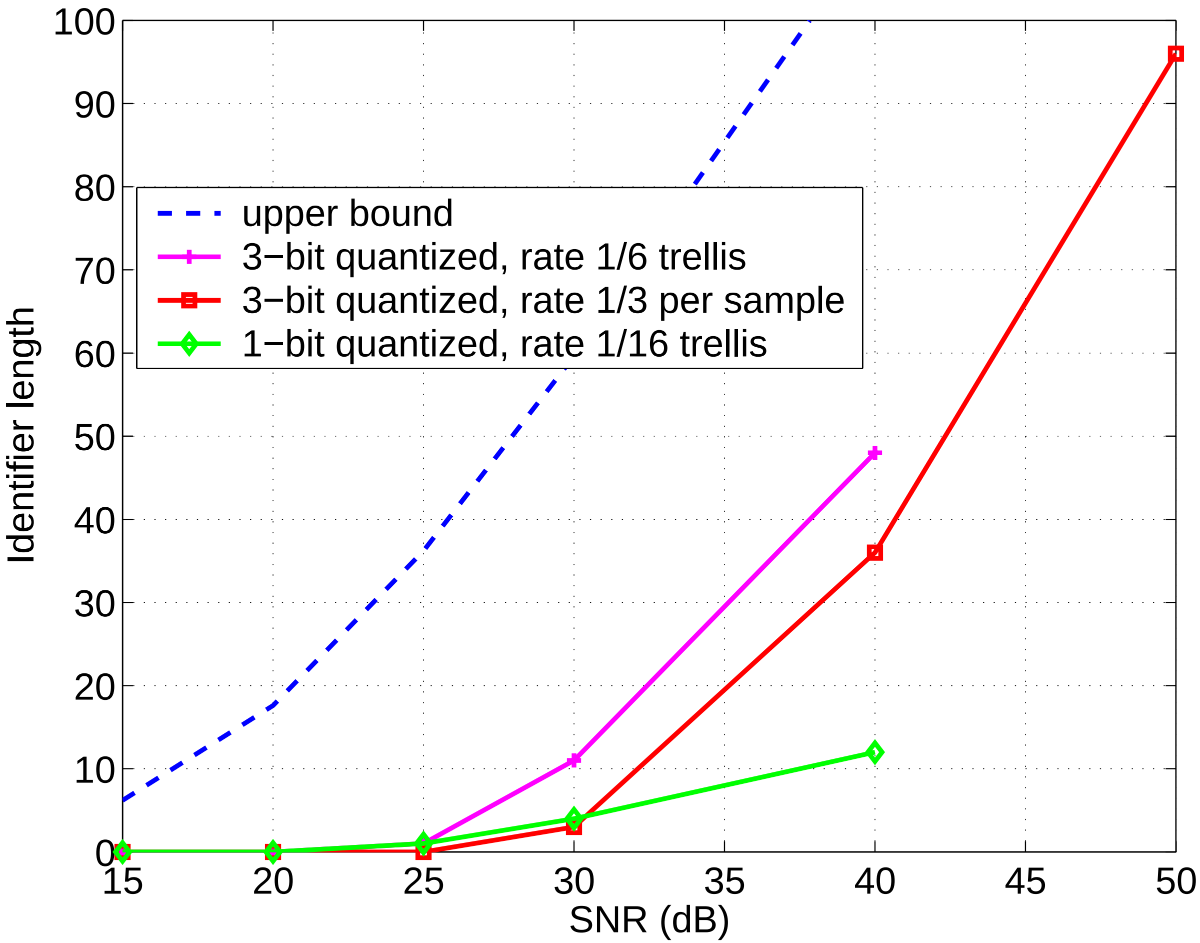


# Impact of Coherence Time

bits/s



# Performance of Actual Schemes


Identifier length
SNR (dB)
upper bound
3−bit quantized, rate 1/6 trellis
3−bit quantized, rate 1/3 per sample
1−bit quantized, rate 1/16 trellis