Security Implications of Implementing Multistate Distance-Bounding Protocols

Jingyi Zhang[1], Anjia Yang[2], Qiao Hu[3] and Gerhard Hancke[1]

1. City University of Hong Kong

2. Jinan University

3. Hunan University

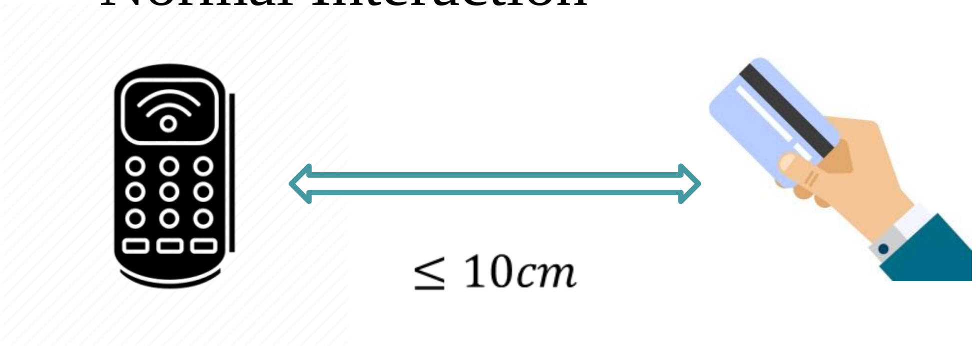
香港城市大學
City University of Hong Kong

Outline

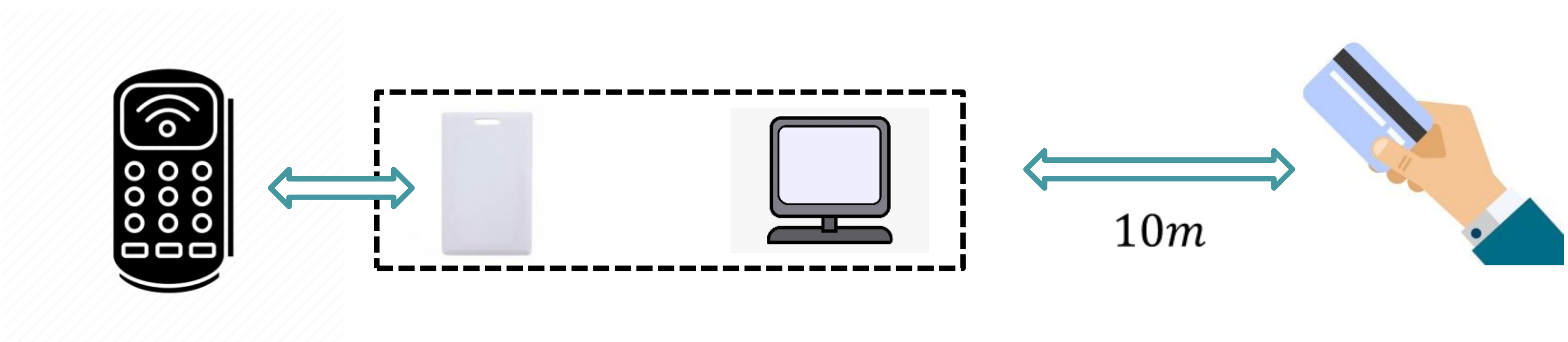
- Authentication and physical proximity
- Distance-bounding protocols
  - Multi-state distance-bounding protocols
  - Security implications of channel implementation
  - Error resilience
- Multi-state distance-bounding channel implications
  - Theoretical vs practical security

Physical Proximity Used for Security and Interaction

- Normal Interaction

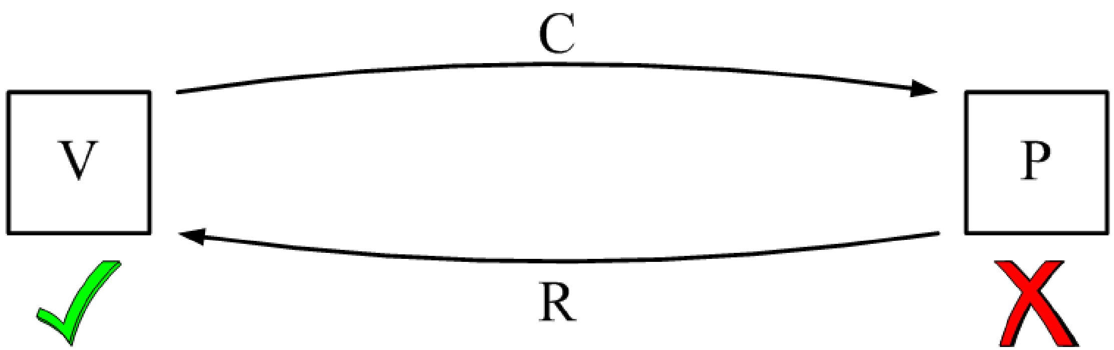


- Relay Attack

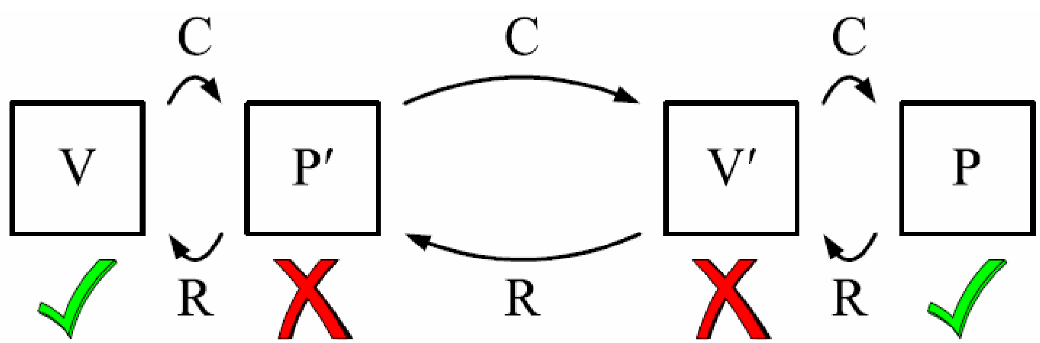


Main Attack Scenarios

- **Distance Fraud:** The prover is fraudulent and tries to convince the verifier that he is closer than is actually the case.



- **Mafia Fraud (Relay):** A fraudulent third party tries to convince the verifier that the prover is in close proximity. Both the verifier and the prover are honest and unaware of the attack.



How Do We Build Such A Protocol?

- Simple echo ?

Verifier	Prover
$C \rightarrow$	$\leftarrow$ C

- Codewords ?

Verifier	Prover
$C \rightarrow$	$\leftarrow$ R

- Challenge response ?

Verifier	Prover
$C \rightarrow$	$\leftarrow$ R= $f\{K,C\}$

It Is Not That Simple

- Response function *f{}* is crucial to protocol success
  - Timed authentication is simplest approach
    - Execute an authentication protocol with a time-out constraint
  - This does not work

$$d = c.\ (t_m - t_d)/2$$

  - Response calculated during timed exchange.
  - Processing delay, and thus bounding estimate, is then variable

- Approaches to fix this
  - Do computation outside timing phase
  - Single bit response calculated using just 1-bit lookup or XOR

Pre-Computation Distance Bounding Protocols

P	V
(hold shared secret key K)	(hold shared secret key K)

$$P \xleftarrow{N_V} V$$

$$P \xrightarrow{N_P} V$$

$$\mathrm{H}(\mathrm{K}, N_V, N_P) \begin{cases} R_1^0, \ldots, R_n^0 \\ R_1^1, \ldots, R_n^1 \end{cases}$$

Start of rapid bit exchange

Repeat n rounds

$$\xleftarrow{c_i} \quad \text{Start a clock}$$

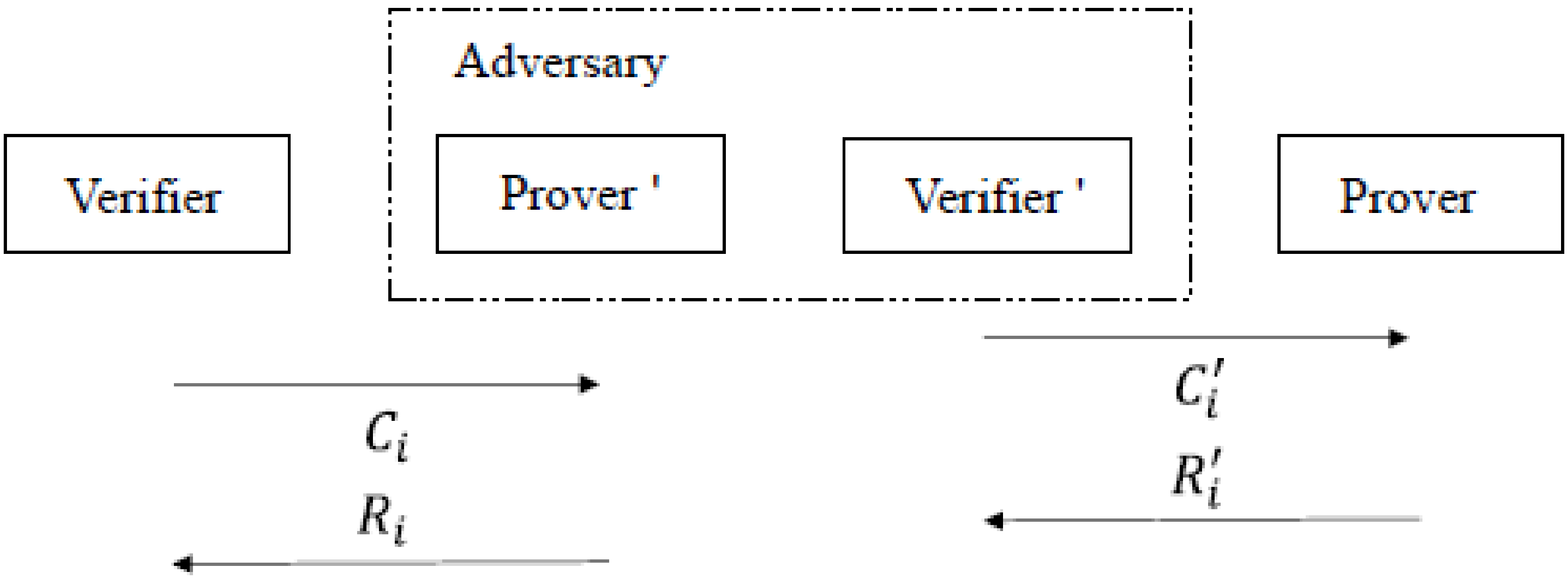
$$\mathrm{r}_i = \begin{cases} R_\mathrm{i}^0, \text{ if } c_i = 0 \\ R_\mathrm{i}^1, \text{ if } c_i = 1 \end{cases} \qquad \xrightarrow{\mathrm{r}_i} \quad \text{End a clock}$$

End of rapid bit exchange

Check correctness of R_i and whether round trip time is within range

Basic Protocol Security Estimates

- Attack success probability
  - Number of challenge-response rounds exchanges n
  - Round ‘win’ chance P_R
  - Attacker expected to win with chance $(P_R)^n$
    - Not necessarily straight forward
    - Example: Mafia fraud in pre-computation $(3/4)^n$



Multistate Distance Bounding Protocol

Verifier (Hold shared key K)

Prover (Hold shared key K)

$$\xrightarrow{N_v}$$

$$\xleftarrow{N_p}$$

$$\mathrm{H}(k, N_v, N_p) = \begin{cases} R_1^0, \ldots, R_i^0, \ldots, R_n^0 \\ \vdots \\ R_1^k, \ldots, R_i^k, \ldots, R_n^k \\ \vdots \\ R_1^{m-1}, \ldots, R_i^{m-1}, \ldots, R_n^{m-1} \end{cases}$$

Start of Fast Bit Exchange step

Repeat n rounds:

Start clock $\xrightarrow{C_i}$

End clock $\xleftarrow{R_i}$

Select $R_i = R_i^k$, if $[C_i]_{10} = \mathrm{k}$

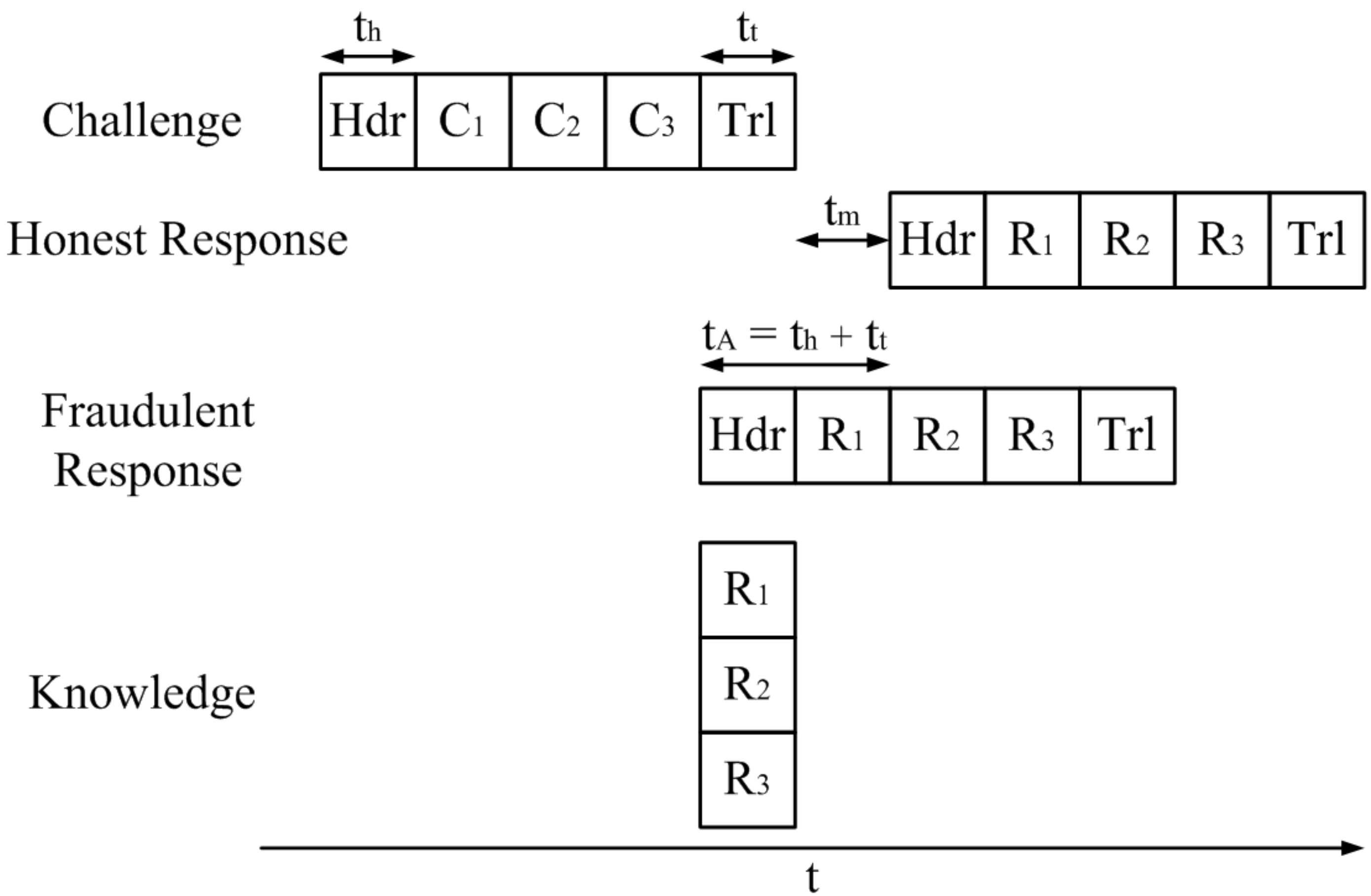
- Multi-state exchanges
- Mafia fraud case

Success Probability: $\left(\frac{2m-1}{m^2}\right)^n$

Potential Issues At The Communication Layer

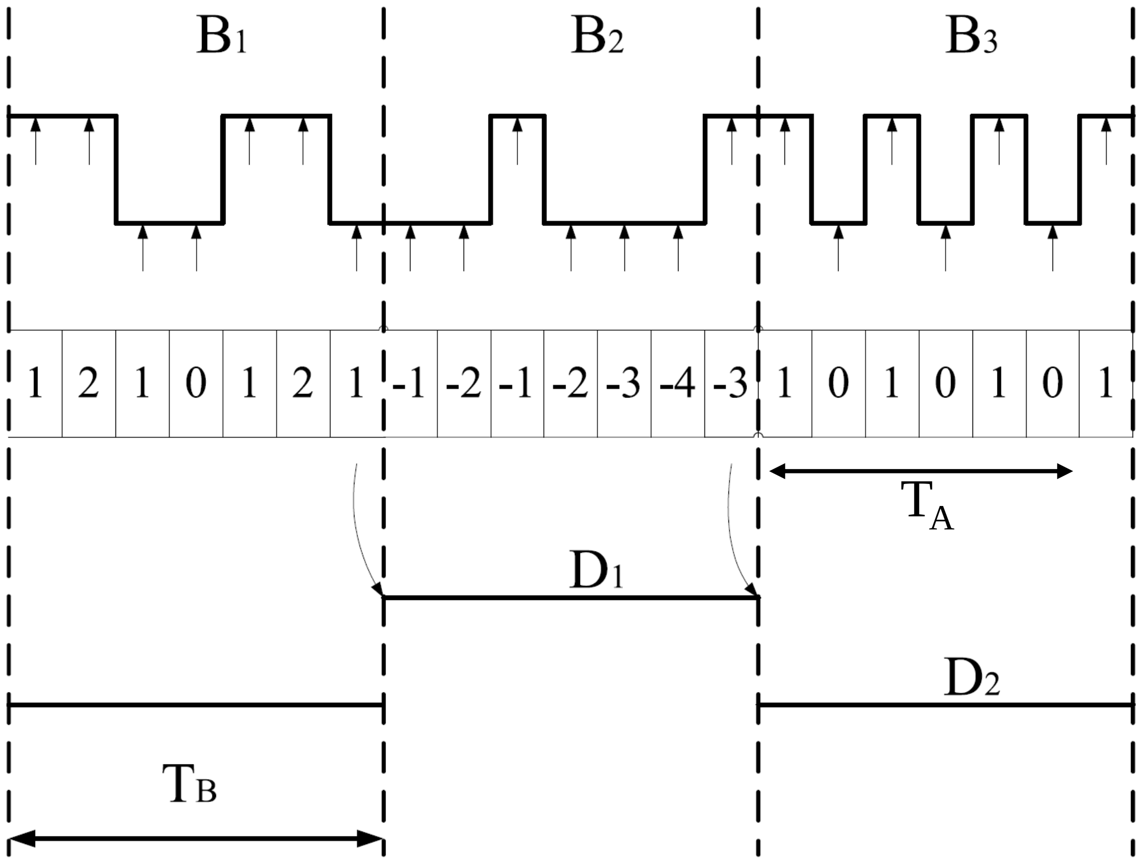
- The communication channel is important for security
  - Distance-bounding requires accurate timing at physical layer.
- Conventional communication channels intended to transmit data reliably.
  - The communication channel introduces latency that an attacker can exploit to circumvent the distance-bound.
- Attacker does not have to follow rules of the protocol or channel.
  - An attacker can use special hardware without restrictions.
- Attacks can be loosely classified into two categories:
  - Attacks at the packet level, e.g. data formatting.
  - Attacks at the physical communication layer, e.g. modulation/coding.

Attack Exploiting Message Format (Extra fields)



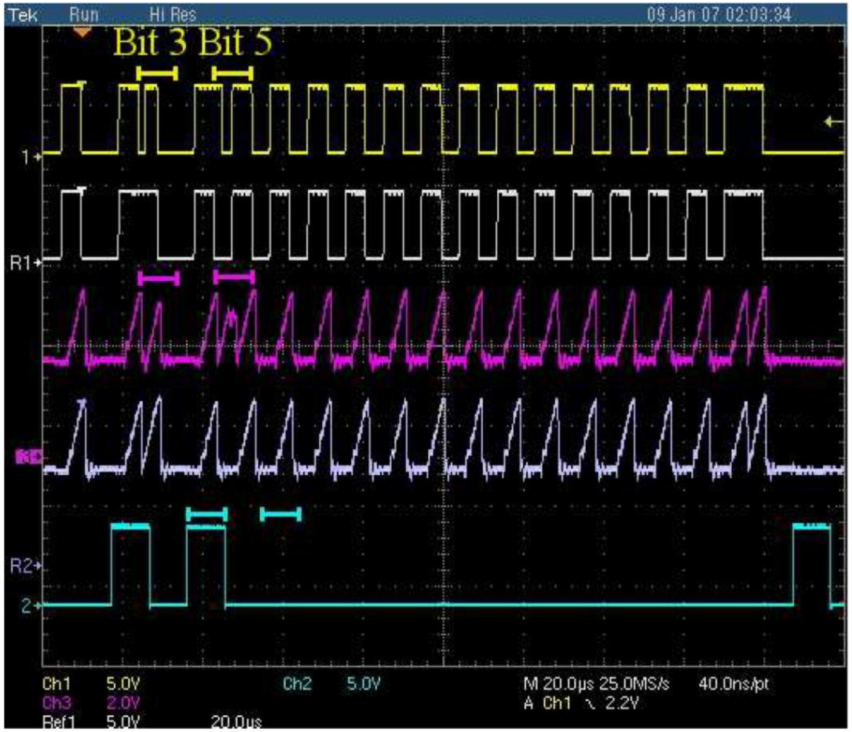
- A dishonest prover can respond pre-emptively
  - Does not have to adhere to ‘rules’ of communication

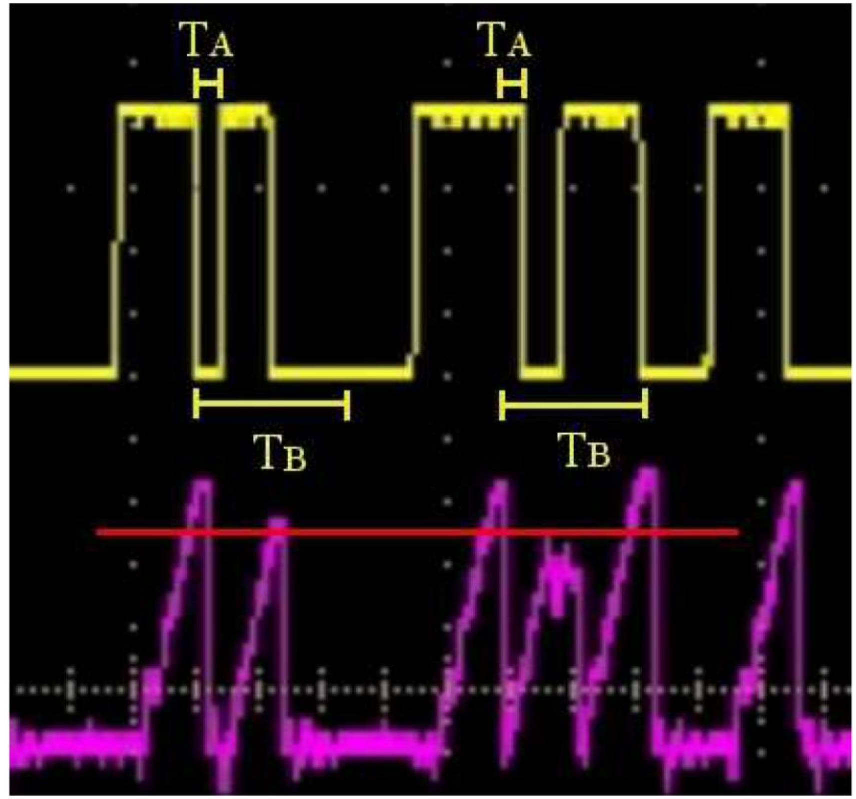
Attack Exploiting Channel Tolerance (Bit decoding)



Majority voting scheme.

Attack Exploiting Channel Tolerance (Bit decoding 2)



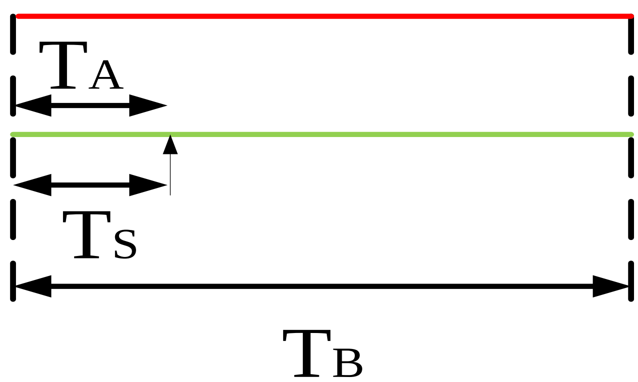


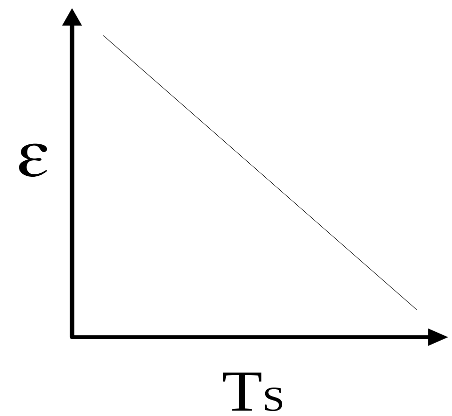
Bit 5: ‘1’ → ‘0’

Bit 3: ‘0’ → ‘1’

Attack Resilience and Errors

- Channel security issues result from reliability measures
- To have more secure DB channels these have to be removed





- As example, early sampling reduces attack time at cost of errors
  - Channel noise, transmission time delay (jitter)

DB with error tolerance and the implications

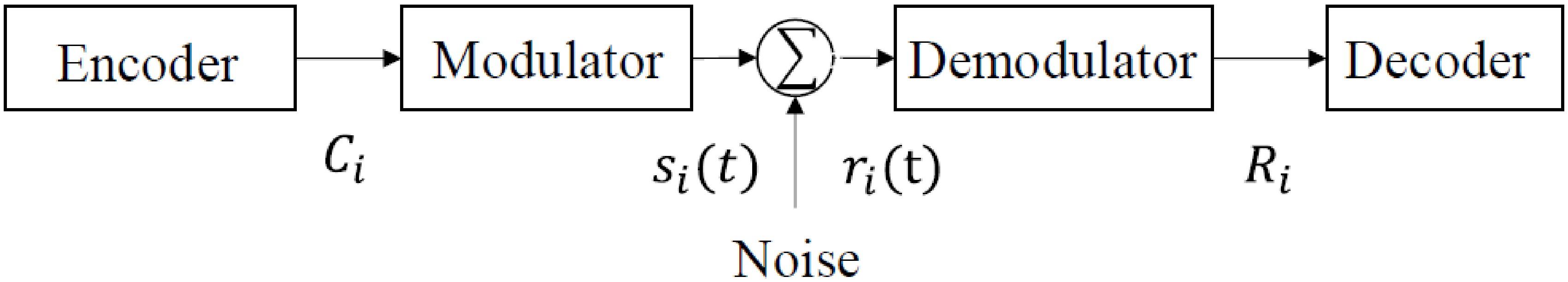
- Distance bounding protocols should ideally allow exchange errors
  - Special channels on resource-constrained devices
  - Environment noise on channel

- Mostly done by specifying an error threshold τ, which is the upper bound on incorrect response acceptable to the verifier.

- A threshold also allows adversaries to pass the protocol by only guessing $n - \tau$ rounds correctly

- Common way to define this threshold in literature is to set $\tau = \omega.n$ where n is number of rounds and ω is bit error probability.

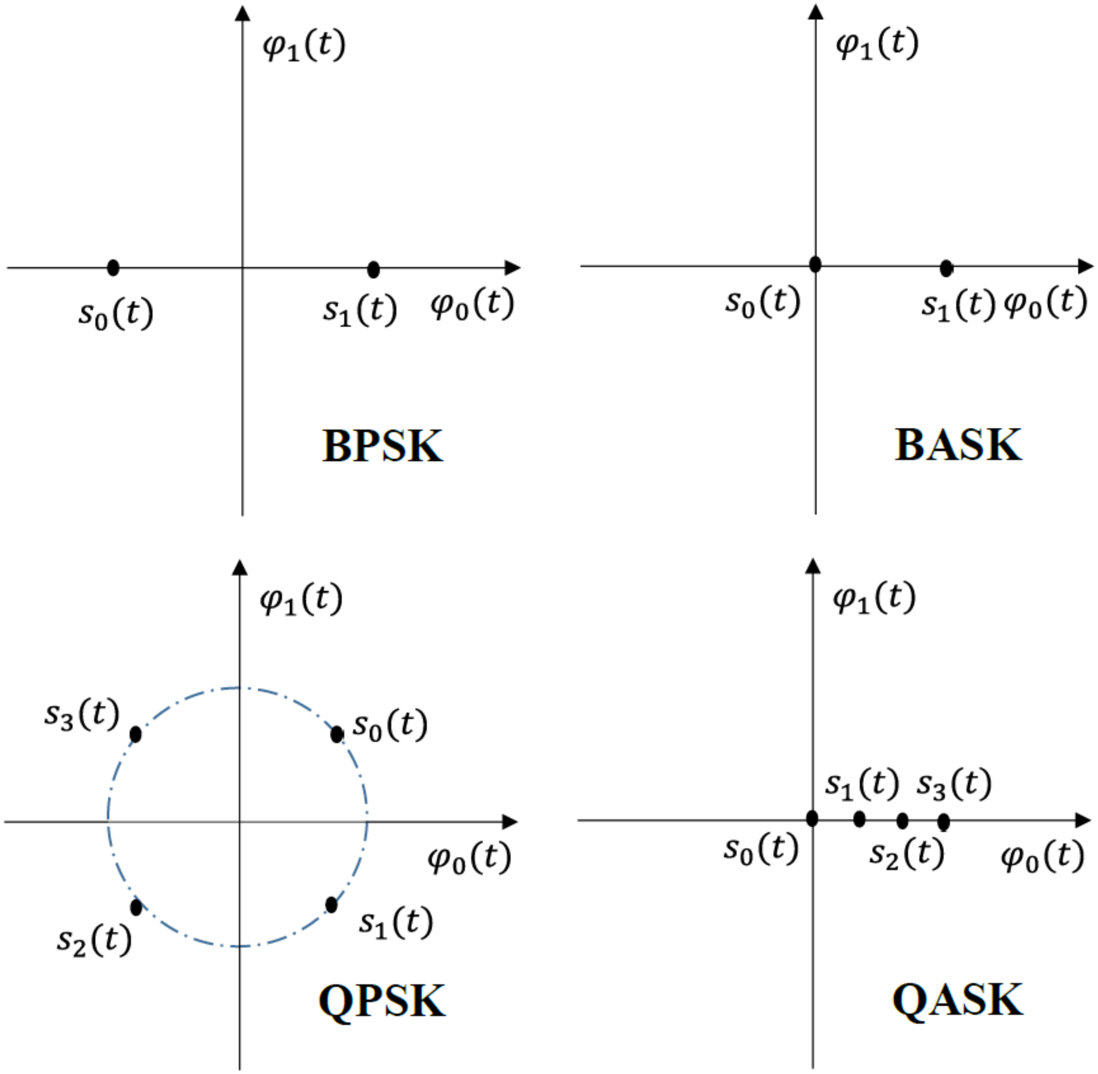
Communication Process and Bit Error Probability



- Noise: Zero mean additive white Gaussian noise (AWGN)

- Resultant transmission bit error rate effected by:
  - Modulation scheme chosen
  - Symbol energy E_S in transmission

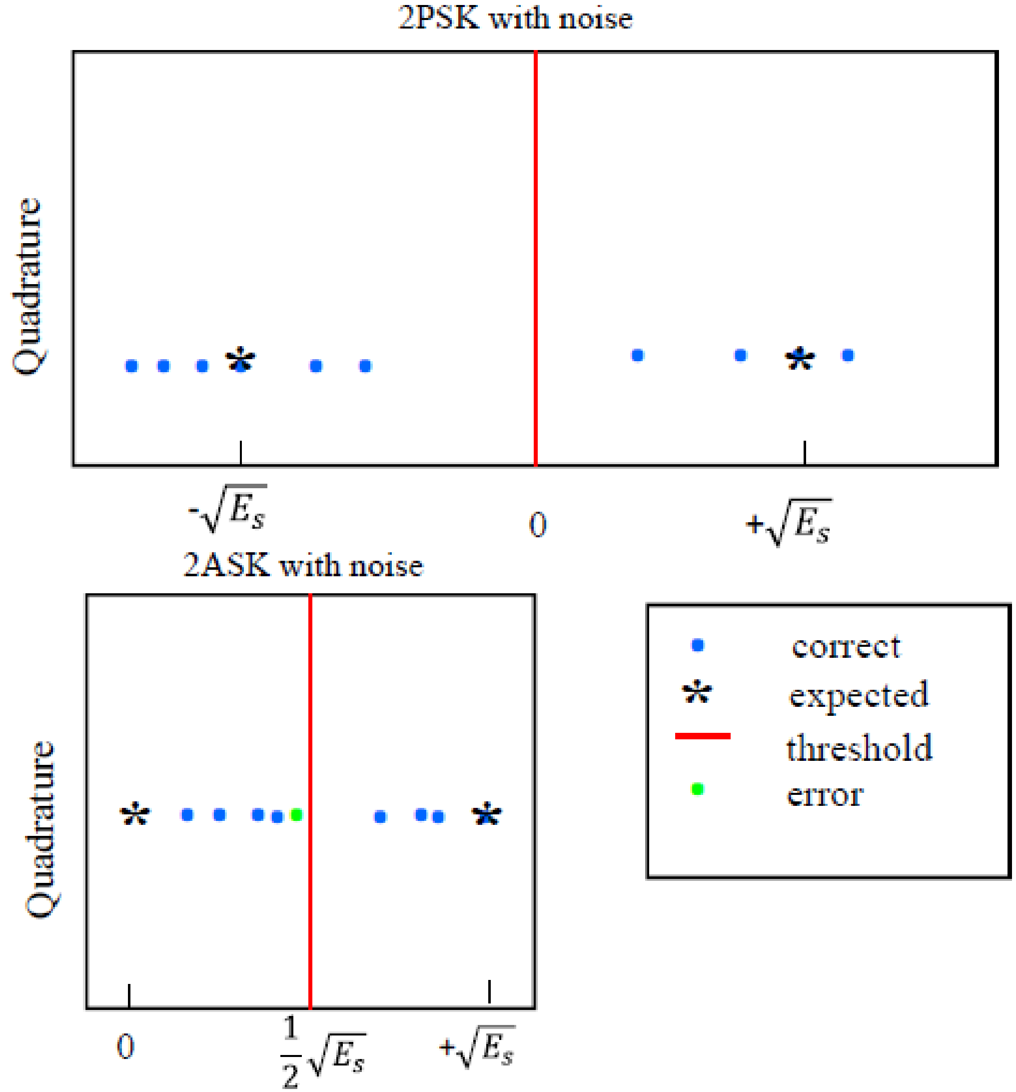
Multistate channels: Symbols



- Symbols have number of specified states
- Symbols can represent more than a bit of data
- For example: 4-state symbol represents 2 bits of data

Multistate communication channels with noise

- If simulating transmissions over an AWGN channel
- Ten received symbols are plotted within the signal space.



Security Implications of Implementing Multistate Symbols

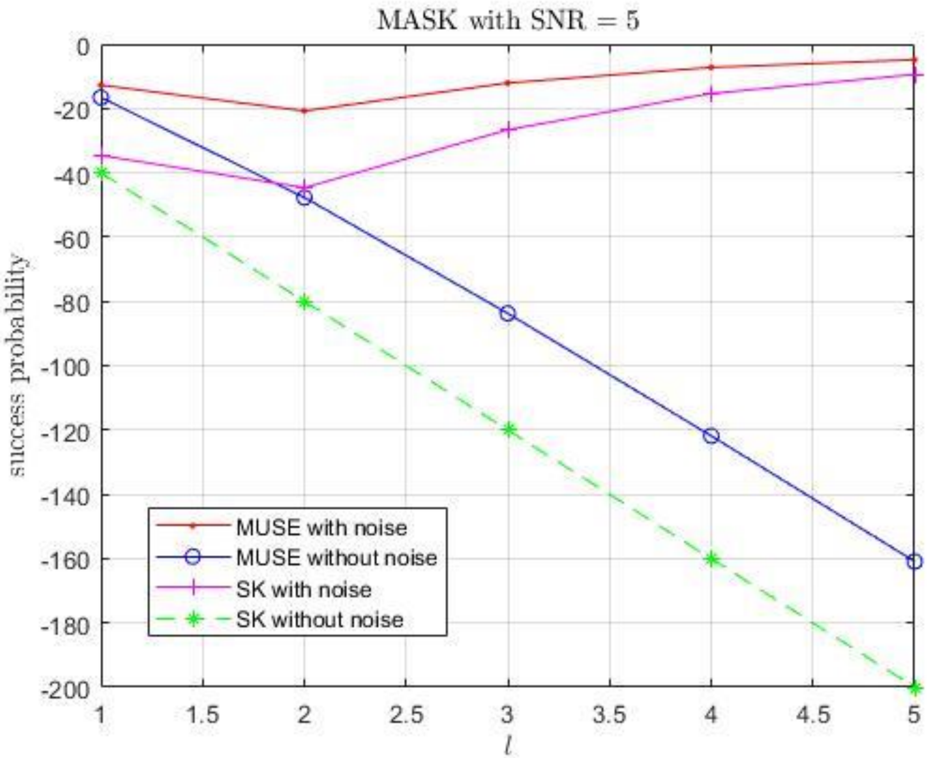
- Mafia fraud success probability:
  - MUSE (no verification) and multistate Swiss-Knife (with verification)

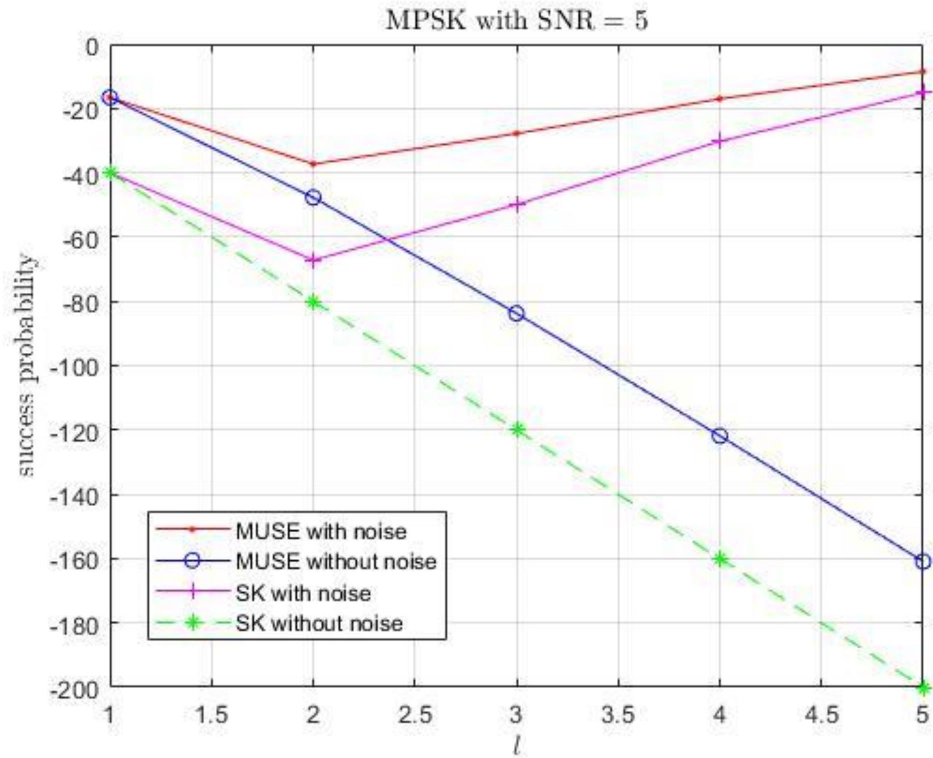
- Consider the noiseless case (the theoretical case) and the noisy case (if a threshold is used to allow for exchange errors).
  - Threshold calculated set as $\tau = \omega.n$

- Evaluate using MASK and MPSK for the channel implementation.
  - Given prevalence in RFID/contactless technology standards

Modulation	$\omega_{SNR=5}$	$\omega_{SNR=10}$	Modulation	$\omega_{SNR=5}$	$\omega_{SNR=10}$
2PSK	0.006	3.87×10^{-6}	2ASK	0.038	7.83×10^{-4}
QPSK	0.074	1.56×10^{-3}	QASK	0.196	0.034
8PSK	0.336	0.087	8ASK	0.510	0.288
16PSK	0.624	0.383	16ASK	0.736	0.588
32PSK	0.805	0.661	32ASK	0.864	0.783

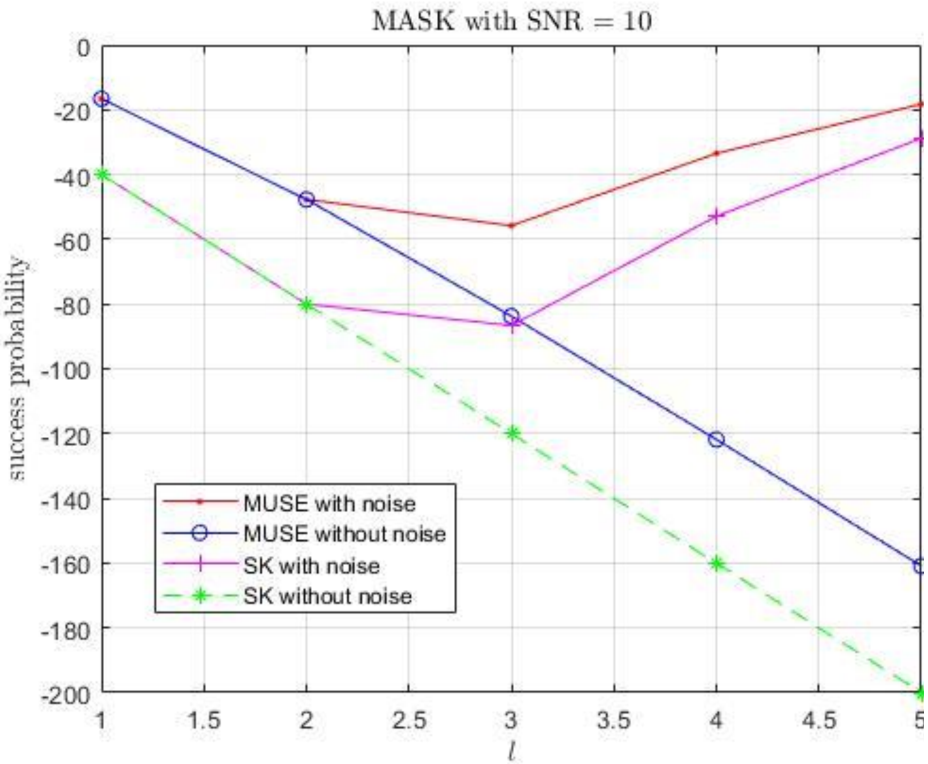
MF Probability for Different Modulation Methods

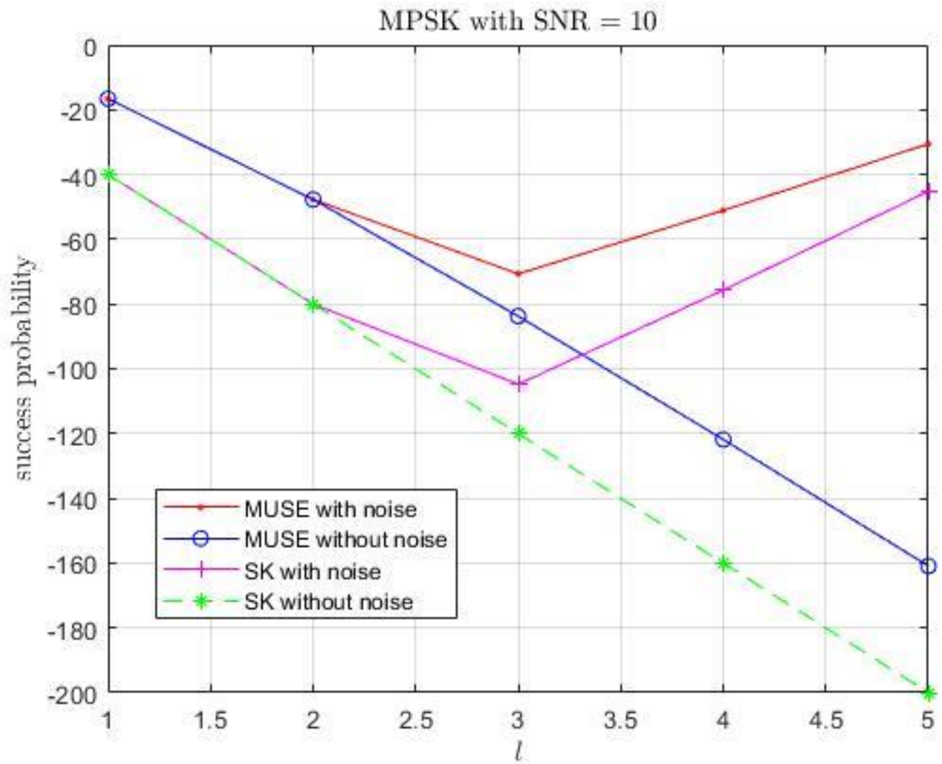




- In noiseless (theoretical) environments, larger *m* result in lower adversary success probabilities as expected.
- In noisy environments the security gain from larger m is counteracted by increased error probability.

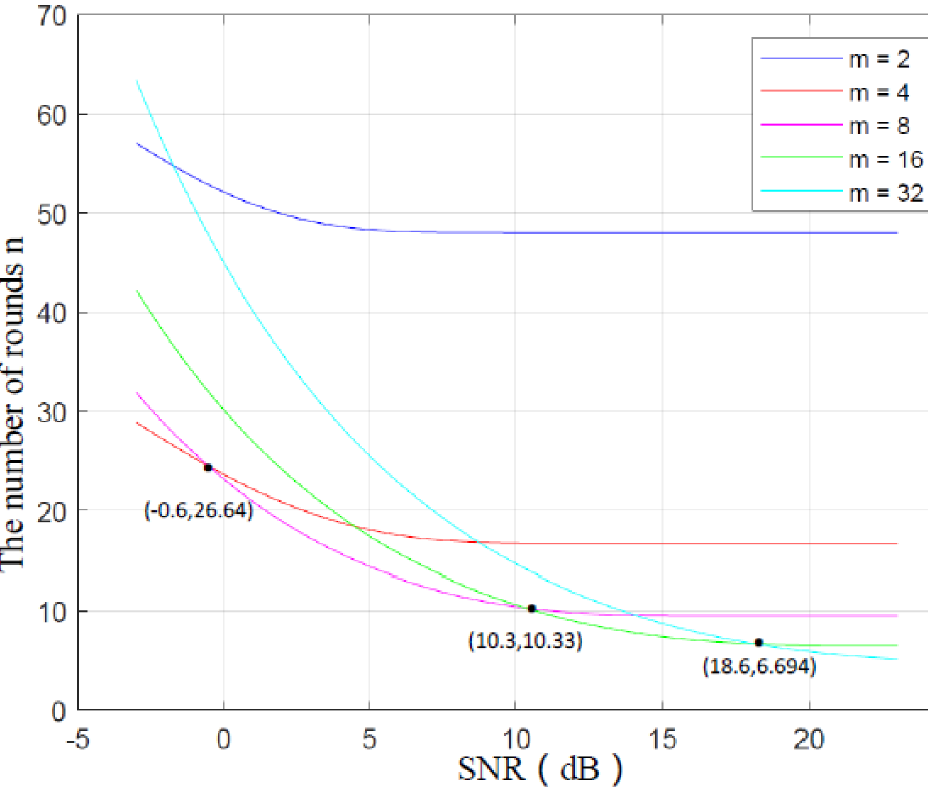
MF Probability for Different Modulation Methods



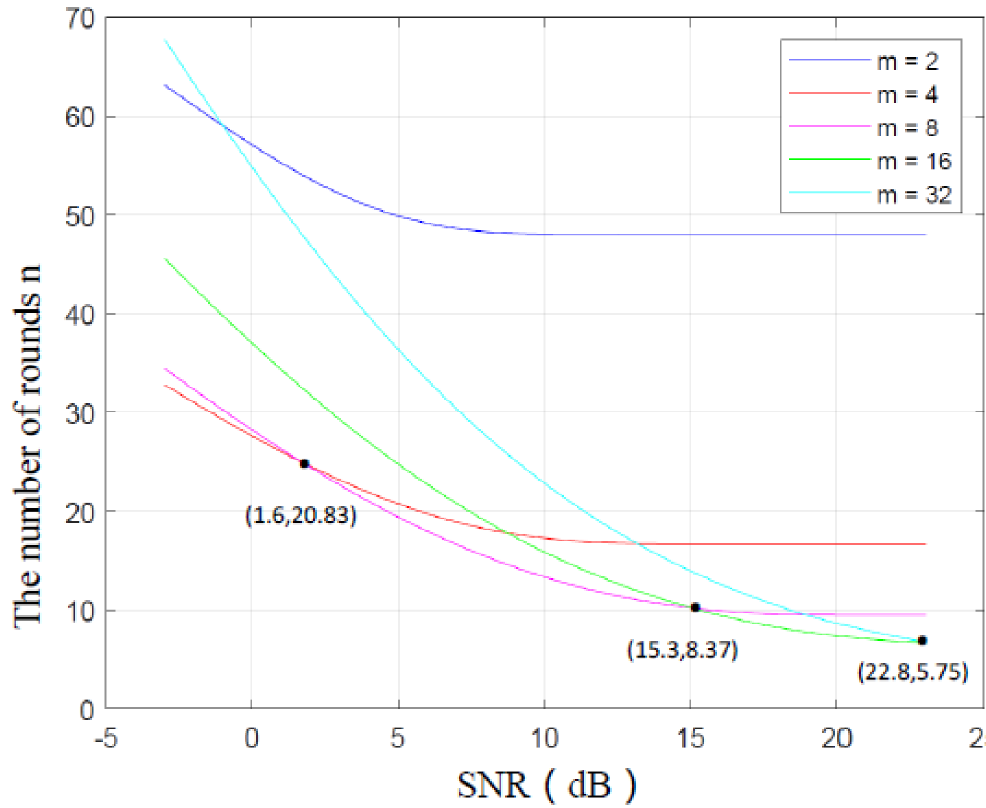


Comment on Choosing Number of Rounds

If we fix the success probability of the attacker, as $P_s = 10^{-5}$, as SNR increased from -3dB to 23dB, the minimum number of rounds n for which different multistate exchange channels achieved this probability for MPSK and MASK are shown below:



MPSK



MASK

Conclusions

- Distance-bounding has a practical use case
  - Protocol design work is quite mature
  - Channel implementation is a challenge
    - Understanding implications of implementations ongoing…
- Investigated multistate DB with common modulation methods
  - Trade-off between states and error resilience - limit on security gains
  - Given an environment, can choose appropriate *m* and modulation
- What to do next…
  - Model other attacks (e.g. distance fraud)
  - Model relationship between *m*, *n* and E_s
    - Expend more energy on fewer rounds to reduce error in higher *m*?

Thank you - questions?