Secrecy for MISO Broadcast Channels with Heterogeneous CSIT

Pritam Mukherjee[1] Ravi Tandon[2] Şennur Ulukuş[1]

[1]University of Maryland, College Park

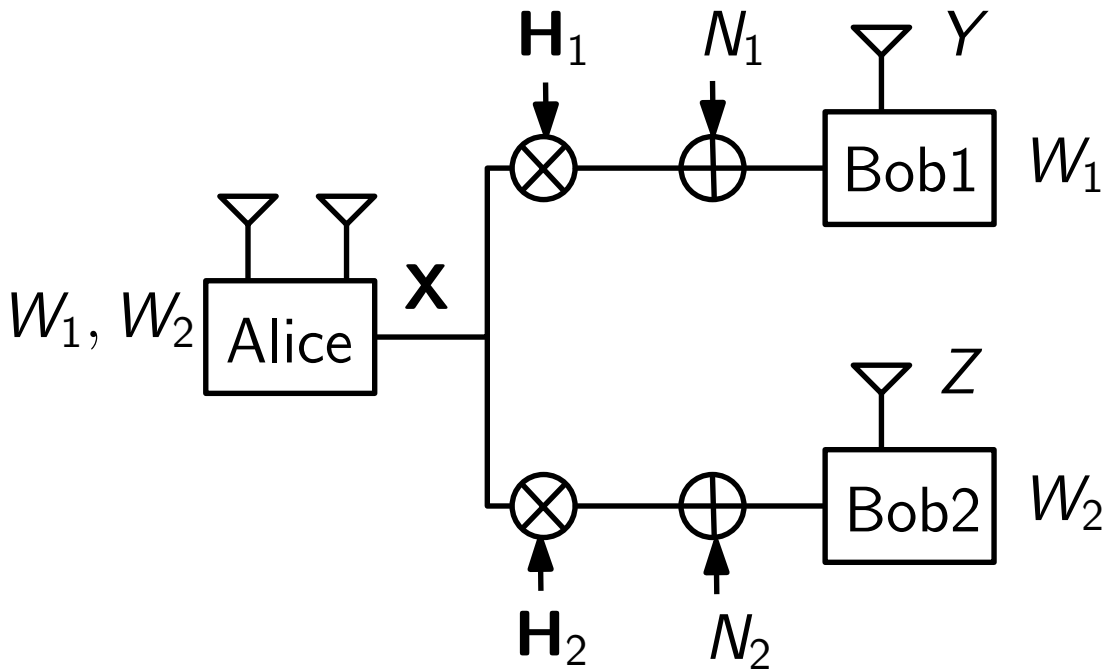
[2]Virginia Tech, Blacksburg

Channel State Information at the Transmitters (CSIT)

- Interference alignment/cancellation in fading wireless networks.
- **Key enabler**: Channel state information (CSI) at the terminals.
- CSI is usually measured at the receivers and fed back to transmitters.
- Assume that the receivers have perfect channel knowledge.
- Availability of CSIT varies: mobility of users, network conditions, etc.
- Thus, CSIT is often *heterogeneous* across users, in practice.
- **This talk:** Focus on the fading MISO broadcast channel.

The MISO Broadcast Channel

- Consider the following fading MISO broadcast channel:



- Assume receivers have full channel knowledge.
- Focus on the availability of CSIT.

Modeling of CSIT

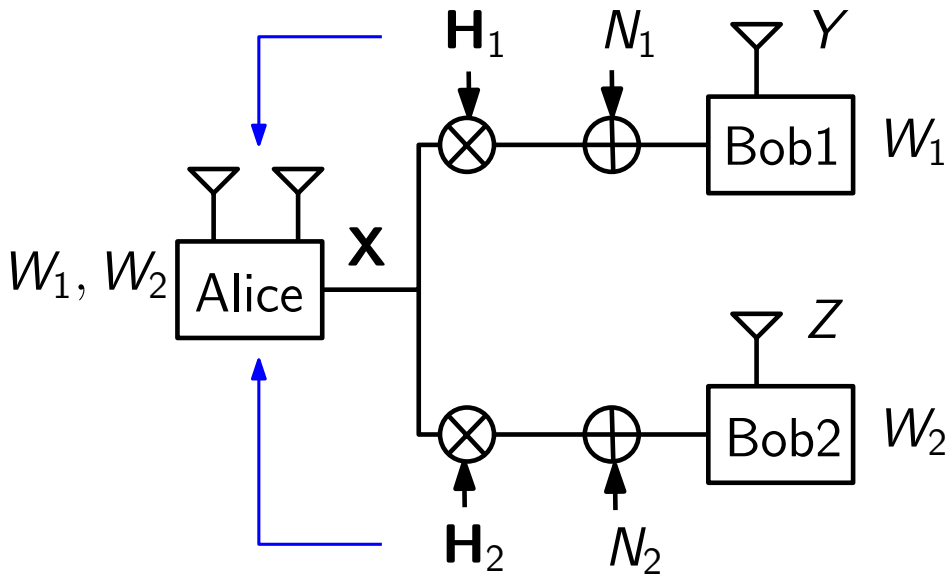
- Two aspects of CSIT: precision and delay.
- In practice, it is usually imprecise and delayed.
- Consider **full precision** and focus on the aspect of delay.
- A simple model of the delay:
  1. perfect (P): The CSIT is available at the start of communication.
  2. delayed (D): The CSIT is available after a delay of coherence time.
  3. none (N): The CSIT of the user is not available.
- With **two** users, define *state* by $I_1 I_2$, where $I_1, I_2 \in \{\text{P, D, N}\}$.
- There can be 9 states: PP, DD, NN, PD, DP, PN, NP, DN, ND.
- *Homogeneous* CSIT states: PP, DD, NN.
- *Heterogeneous* CSIT states: PD, DP, PN, NP, DN, ND.

Impact of CSIT

Degrees of Freedom			
CSIT states		Without Secrecy	With Secrecy
Homogeneous	PP DD NN		
Heterogeneous	PD PN DN		

Homogeneous CSIT

- For the MISO broadcast channel:

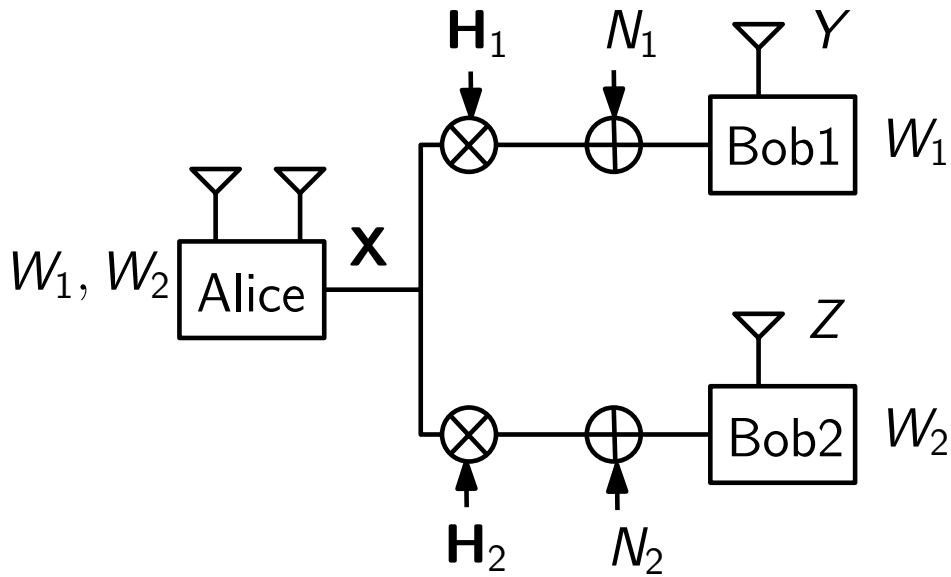


- With perfect CSIT (P) from both users, sum d.o.f =2.

[a] Maddah-Ali, Tse (2010)

Homogeneous CSIT

- For the MISO broadcast channel:

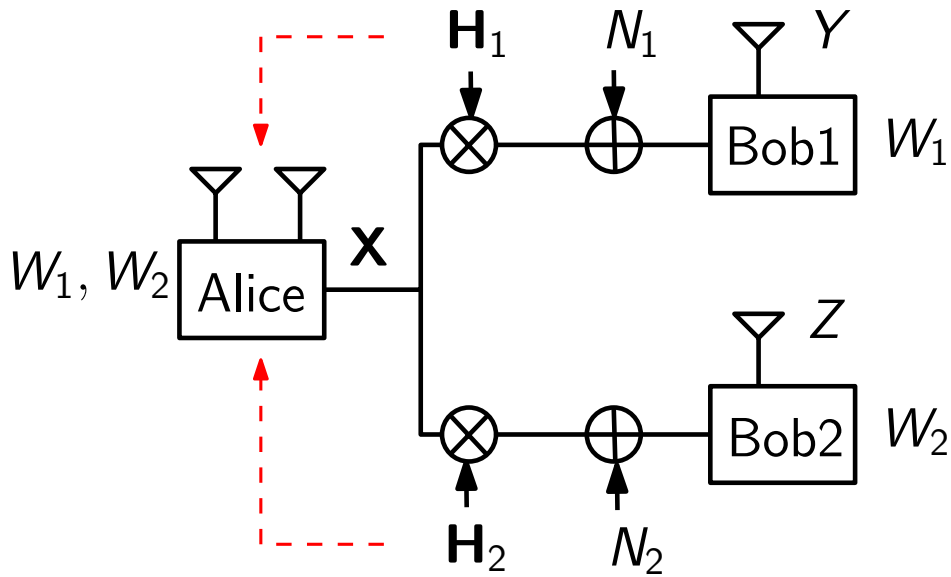


- With perfect CSIT (P) from both users, sum d.o.f =2.
- With no CSIT (N), the sum degrees of freedom (d.o.f.) is 1.

[a] Maddah-Ali, Tse (2010)

Homogeneous CSIT

- For the MISO broadcast channel:

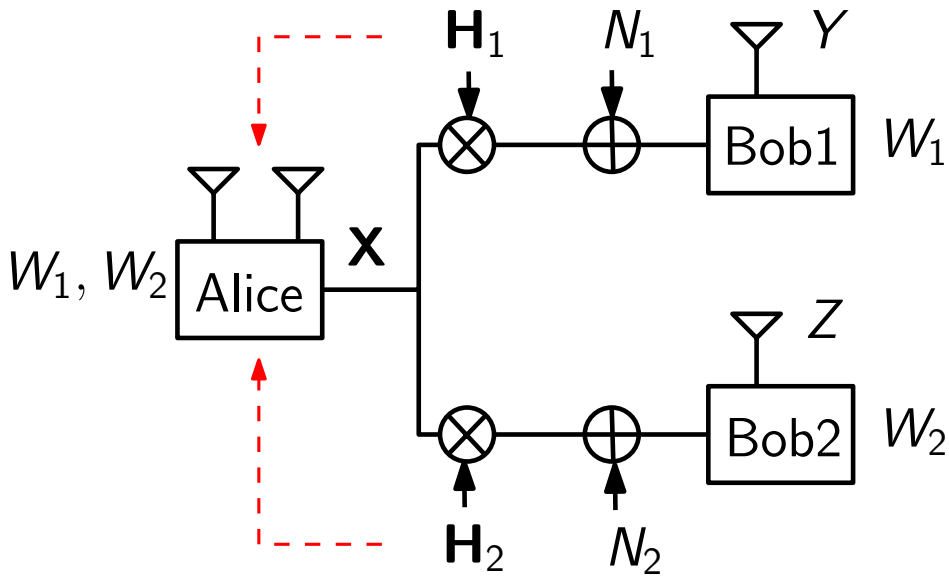


- With perfect CSIT (P) from both users, sum d.o.f =2.
- With no CSIT (N), the sum degrees of freedom (d.o.f.) is 1.
- With delayed[a] CSIT (D) from both users, sum d.o.f = $\frac{4}{3}$.

[a] Maddah-Ali, Tse (2010)

Homogeneous CSIT

- For the MISO broadcast channel:



- With perfect CSIT (P) from both users, sum d.o.f =2.
- With no CSIT (N), the sum degrees of freedom (d.o.f.) is 1.
- With delayed[a] CSIT (D) from both users, sum d.o.f = $\frac{4}{3}$.

Even completely outdated CSIT is useful!

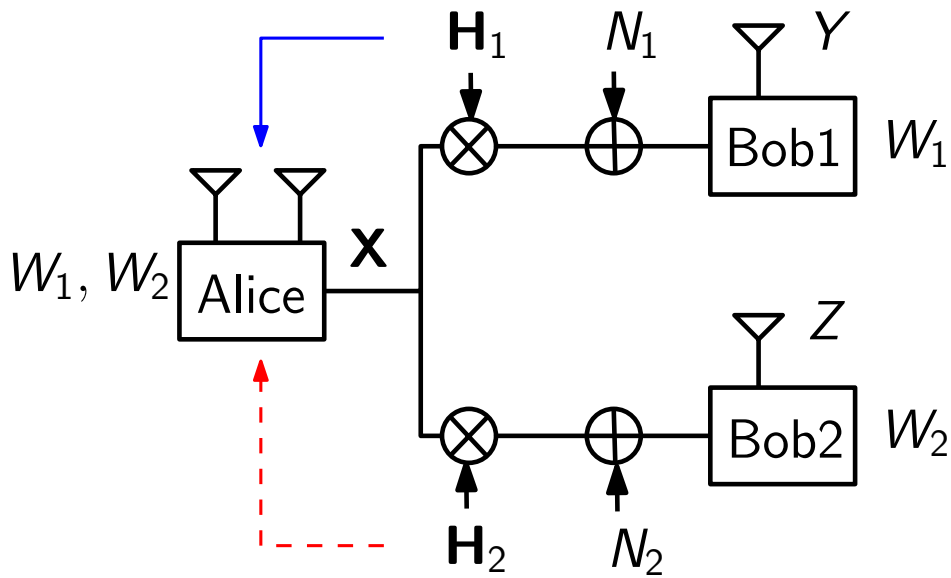
[a] Maddah-Ali, Tse (2010)

Impact of CSIT

Degrees of Freedom			
CSIT states		Without Secrecy	With Secrecy
Homogeneous	PP	2	
	DD	4/3	
	NN	1	
Heterogeneous	PD		
	PN		
	DN		

Heterogeneous CSIT

- The CSIT supplied by the two users may be different w.r.t. delay.
- This may be due to network conditions or mobility of users.

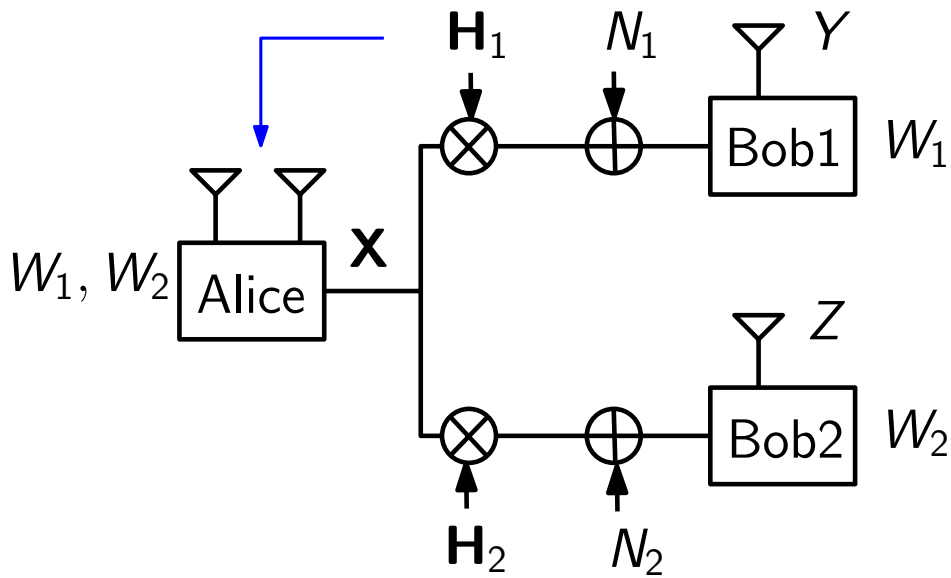


- With perfect and delayed[a] CSIT from users (PD): Sum d.o.f $= \frac{3}{2}$.

[a] Maleki et al. (2012)
[b] Davoodi, Jafar (2014)

Heterogeneous CSIT

- The CSIT supplied by the two users may be different w.r.t. delay.
- This may be due to network conditions or mobility of users.

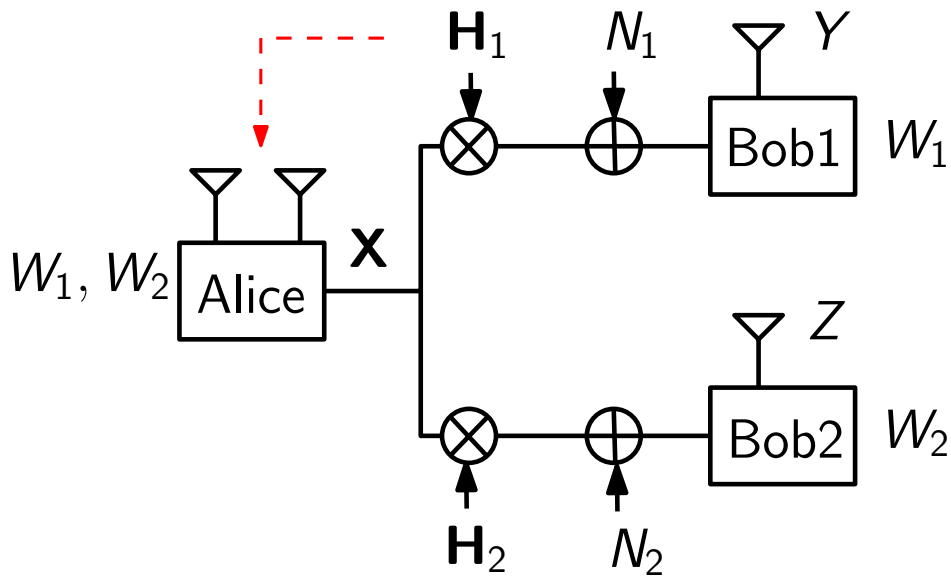


- With perfect and delayed[a] CSIT from users (PD): Sum d.o.f $= \frac{3}{2}$.
- With perfect and no[b] CSIT from the users (PN): Sum d.o.f $= 1$.

[a] Maleki et al. (2012)
[b] Davoodi, Jafar (2014)

Heterogeneous CSIT

- The CSIT supplied by the two users may be different w.r.t. delay.
- This may be due to network conditions or mobility of users.



- With perfect and delayed[a] CSIT from users (PD): Sum d.o.f $= \frac{3}{2}$.
- With perfect and no[b] CSIT from the users (PN): Sum d.o.f $= 1$.
- With delayed and no CSIT from the users (DN): Sum d.o.f $= 1$.

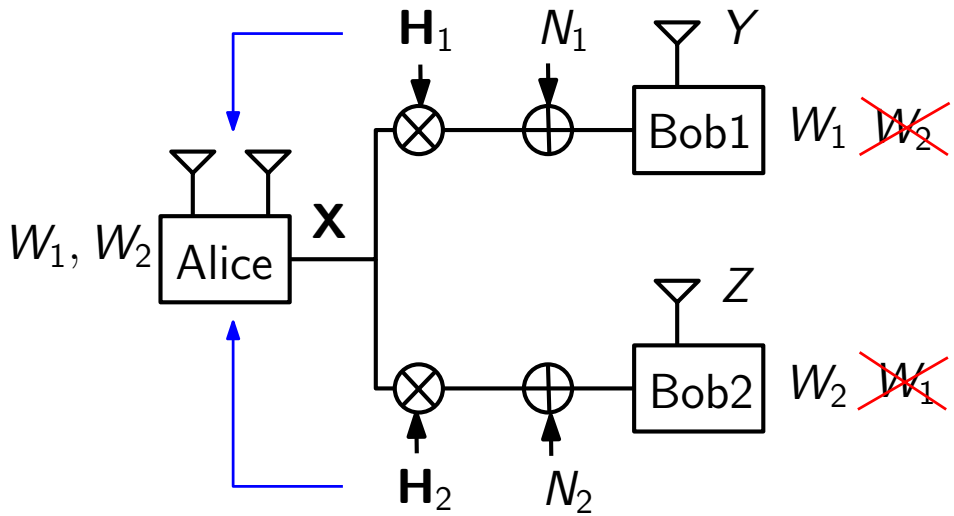
[a] Maleki et al. (2012)
[b] Davoodi, Jafar (2014)

Impact of CSIT

Degrees of Freedom			
CSIT states		Without Secrecy	With Secrecy
Homogeneous	PP	2	
	DD	4/3	
	NN	1	
Heterogeneous	PD	3/2	
	PN	1	
	DN	1	

Security aspects

- We focus on the security aspect of the problem.
- Consider the MISO Broadcast channel with confidential messages (BCCM).

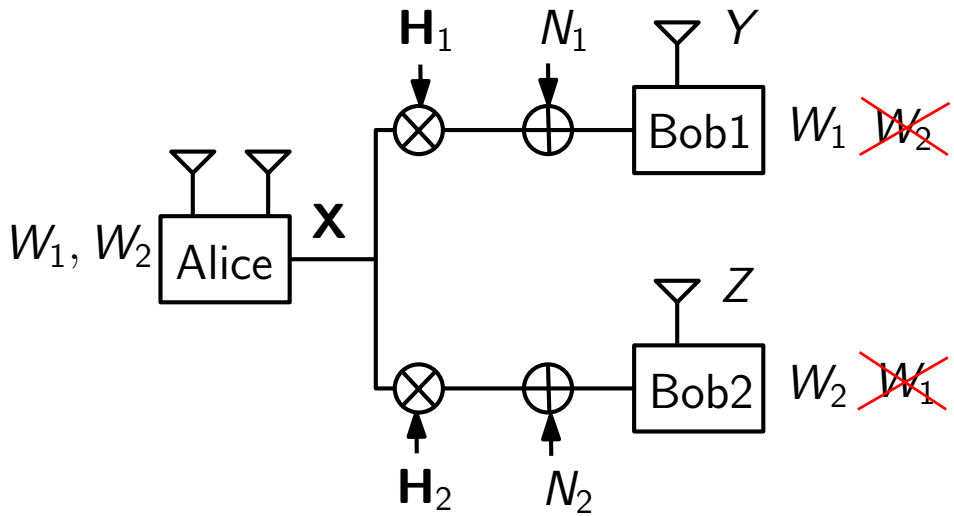


- Perfect CSIT (P) from both users, sum s.d.o.f. $= 2$.

[a] S. Yang et al. (2013)

Security aspects

- We focus on the security aspect of the problem.
- Consider the MISO Broadcast channel with confidential messages (BCCM).

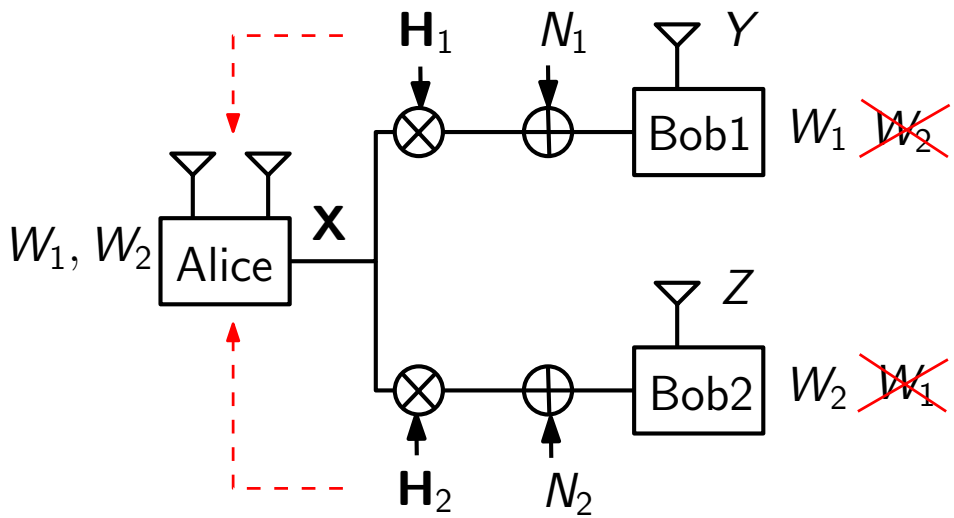


- Perfect CSIT (P) from both users, sum s.d.o.f. $= 2$.
- No CSIT (N): statistically equivalent users; sum s.d.o.f.$= 0$.

[a] S. Yang et al. (2013)

Security aspects

- We focus on the security aspect of the problem.
- Consider the MISO Broadcast channel with confidential messages (BCCM).



- Perfect CSIT (P) from both users, sum s.d.o.f. $= 2$.
- No CSIT (N): statistically equivalent users; sum s.d.o.f.$= 0$.
- Delayed[a] CSIT (D) from both users: sum s.d.o.f. $= 1$.

[a] S. Yang et al. (2013)

Impact of CSIT

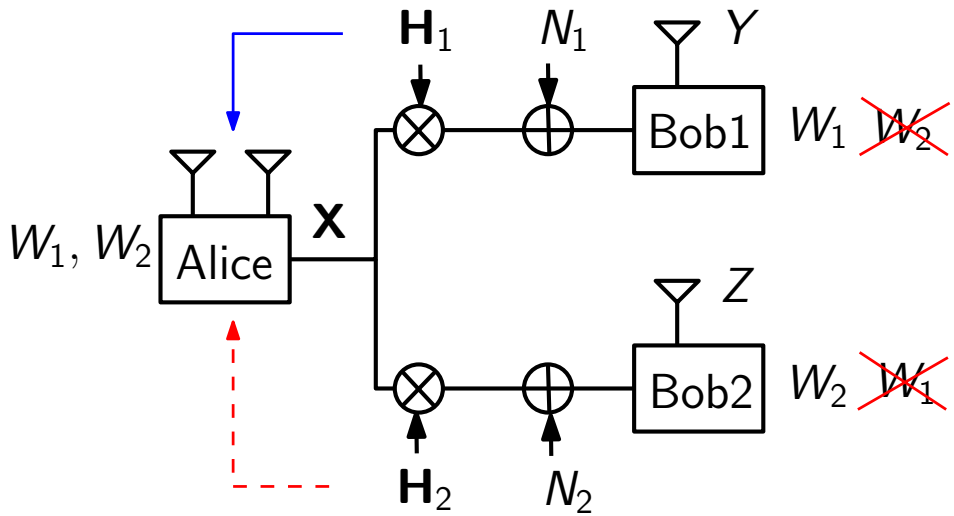
Degrees of Freedom			
CSIT states		Without Secrecy	With Secrecy
Homogeneous	PP	2	2
	DD	4/3	1
	NN	1	0
Heterogeneous	PD	3/2	
	PN	1	
	DN	1	

Impact of CSIT

Degrees of Freedom			
CSIT states		Without Secrecy	With Secrecy
Homogeneous	PP	2	2
	DD	4/3	1
	NN	1	0
Heterogeneous	PD	3/2	THIS TALK!
	PN	1	
	DN	1	

Our Results: Security with Heterogeneous CSIT

- Consider the MISO BCCM with heterogeneous CSIT.

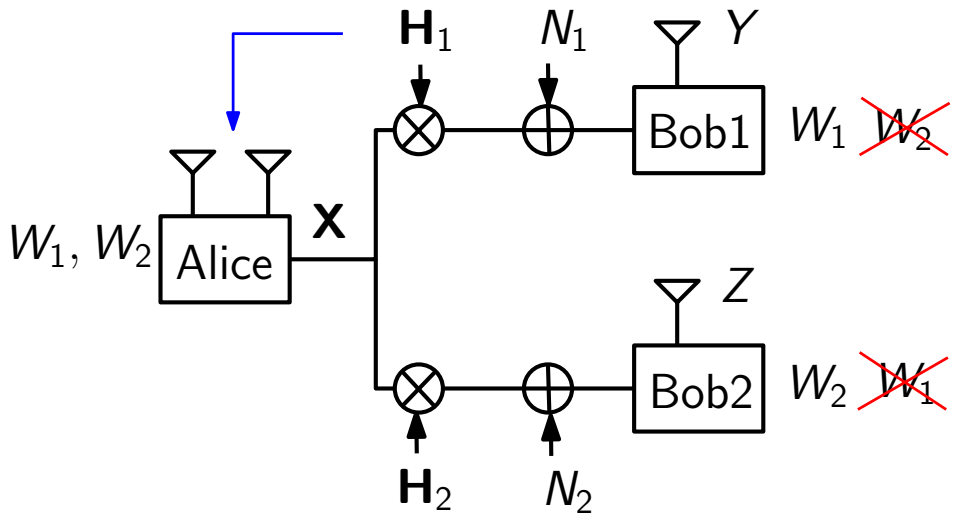


- With perfect and delayed CSIT from users (PD): Sum s.d.o.f $= 1$.

[a] Lashgari, Avestimehr (2014) with *linear* encoding schemes

Our Results: Security with Heterogeneous CSIT

- Consider the MISO BCCM with heterogeneous CSIT.

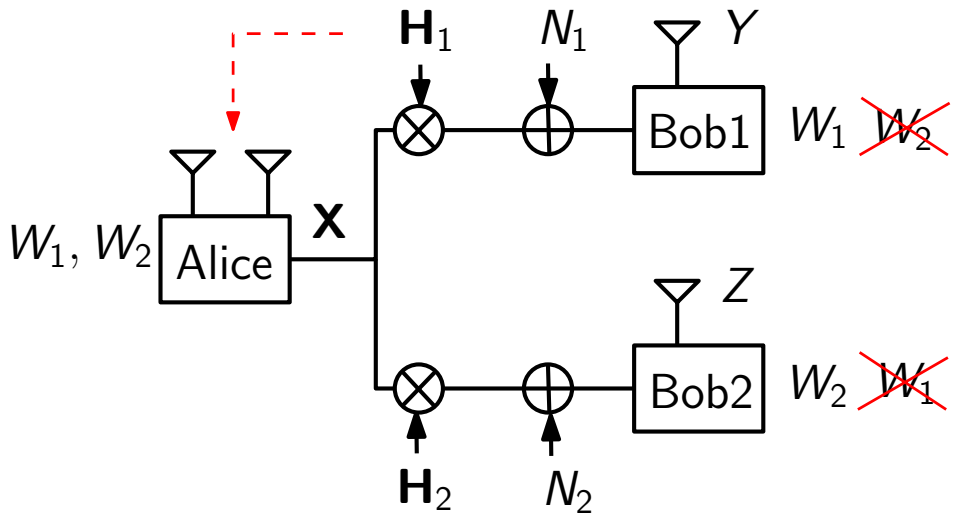


- With perfect and delayed CSIT from users (PD): Sum s.d.o.f $= 1$.
- With perfect and no CSIT from the users (PN): Sum d.o.f $= 1$.

[a] Lashgari, Avestimehr (2014) with *linear* encoding schemes

Our Results: Security with Heterogeneous CSIT

- Consider the MISO BCCM with heterogeneous CSIT.



- With perfect and delayed CSIT from users (PD): Sum s.d.o.f $= 1$.
- With perfect and no CSIT from the users (PN): Sum d.o.f $= 1$.
- With delayed and no CSIT[a] from the users (DN): Sum d.o.f $= \frac{1}{2}$.

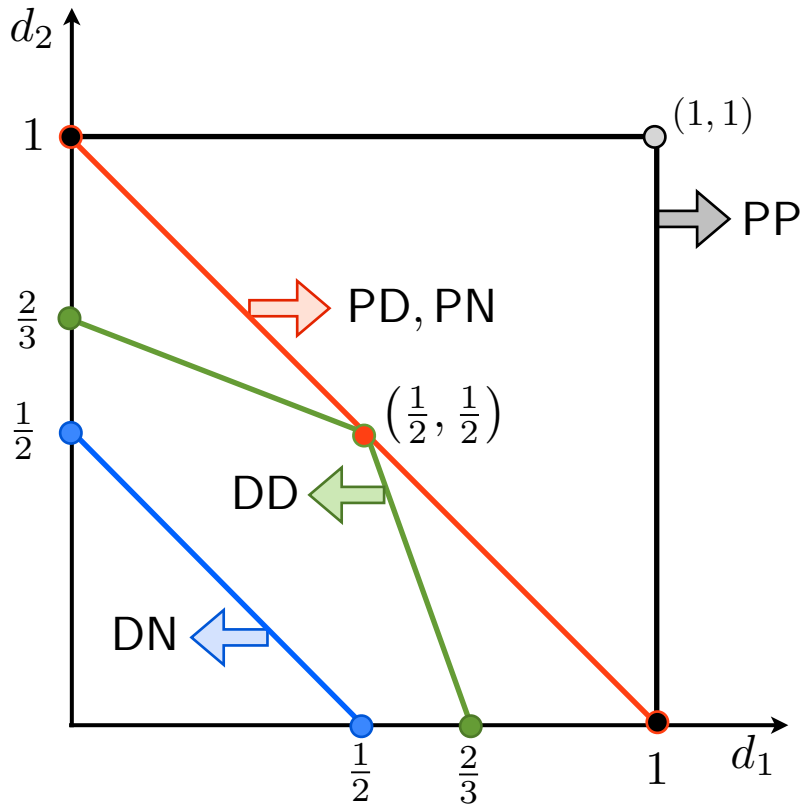
[a] Lashgari, Avestimehr (2014) with *linear* encoding schemes

Impact of CSIT

Degrees of Freedom			
CSIT states		Without Secrecy	With Secrecy
Homogeneous	PP	2	2
	DD	4/3	1
	NN	1	0
Heterogeneous	PD	3/2	1
	PN	1	1
	DN	1	1/2

Our Results (Contd.)

- The optimal s.d.o.f. regions are:



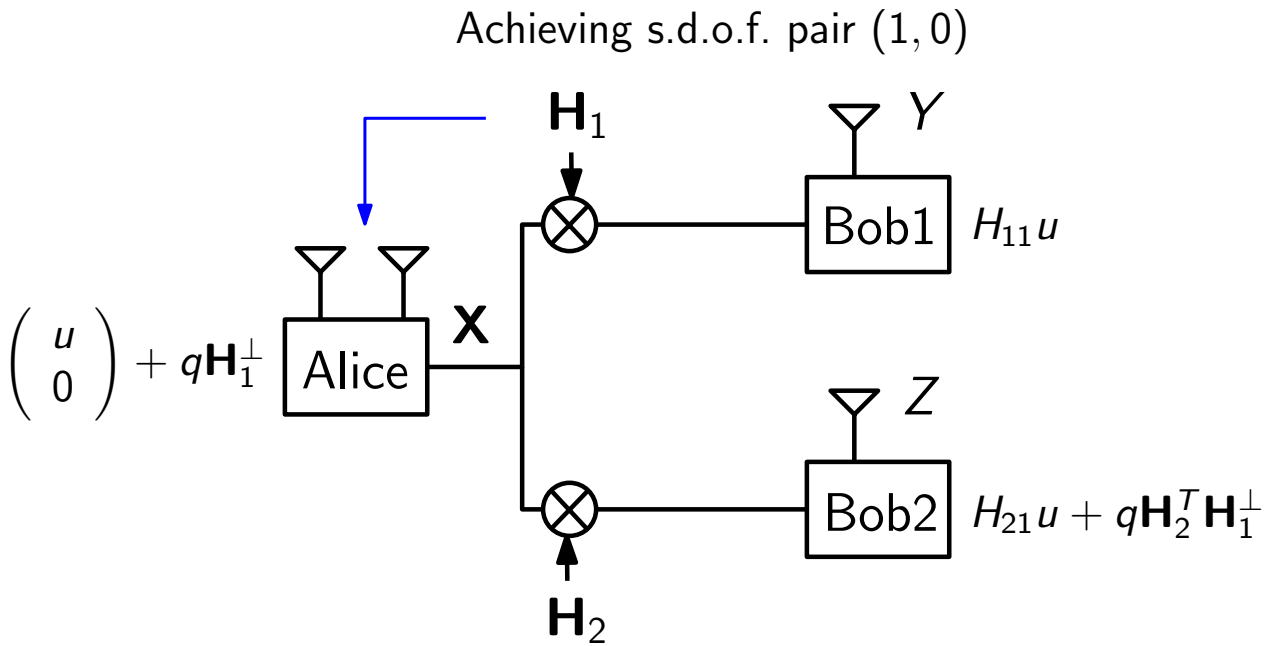
Remarks

- The PD and PN states have same s.d.o.f. region.
  - When one user provides perfect CSIT, delayed CSIT from the other is not useful.
- The PD and DD states have the same optimal sum s.d.o.f. of 1.
  - When one user provides delayed CSIT, perfect CSIT from the other is not useful from the sum s.d.o.f. perspective.
  - However, this is **not** true from a s.d.o.f. *region* perspective.
- Benefits of *alternating* CSIT:
  - Alternating states PD and DP[a], optimal sum s.d.o.f. $= \frac{3}{2}$. Benefit!
  - Alternating states DN and ND[b], optimal sum s.d.o.f. $= 1$. Benefit!
  - Alternating states PN and NP[b], optimal sum s.d.o.f. $= 1$. No Benefit

[a] Mukherjee, Tandon, Ulukus (2014)
[b] Mukherjee, Tandon, Ulukus (2015)

Achievable Schemes

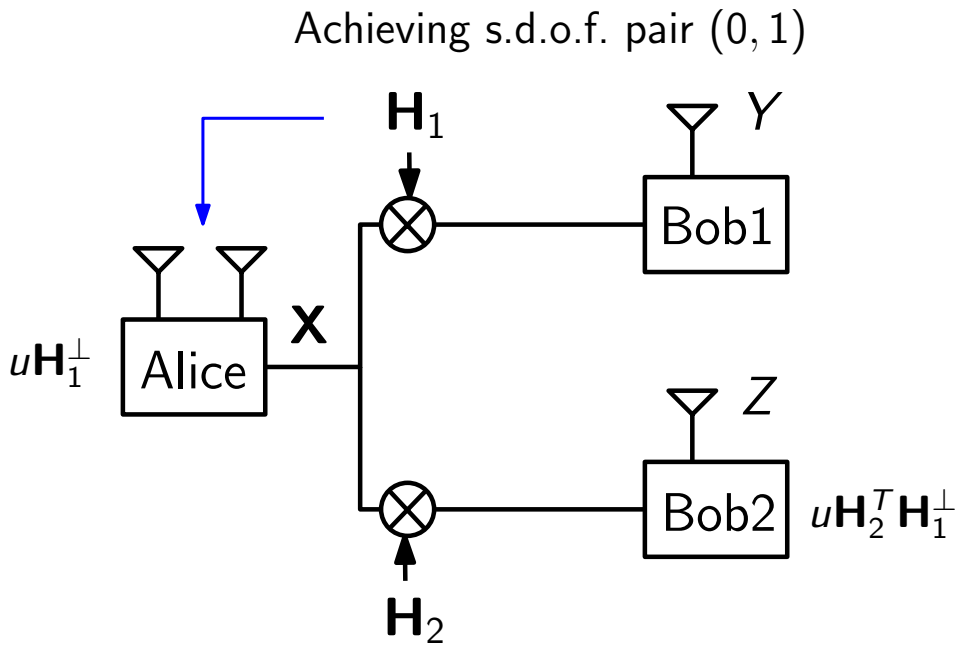
- A scheme for state PN also suffices for state PD.
- **Schemes for state PN**: Achieve s.d.o.f. pairs $(0, 1)$ and $(1, 0)$:



- The full region is achieved by time-sharing between these points.

Achievable Schemes

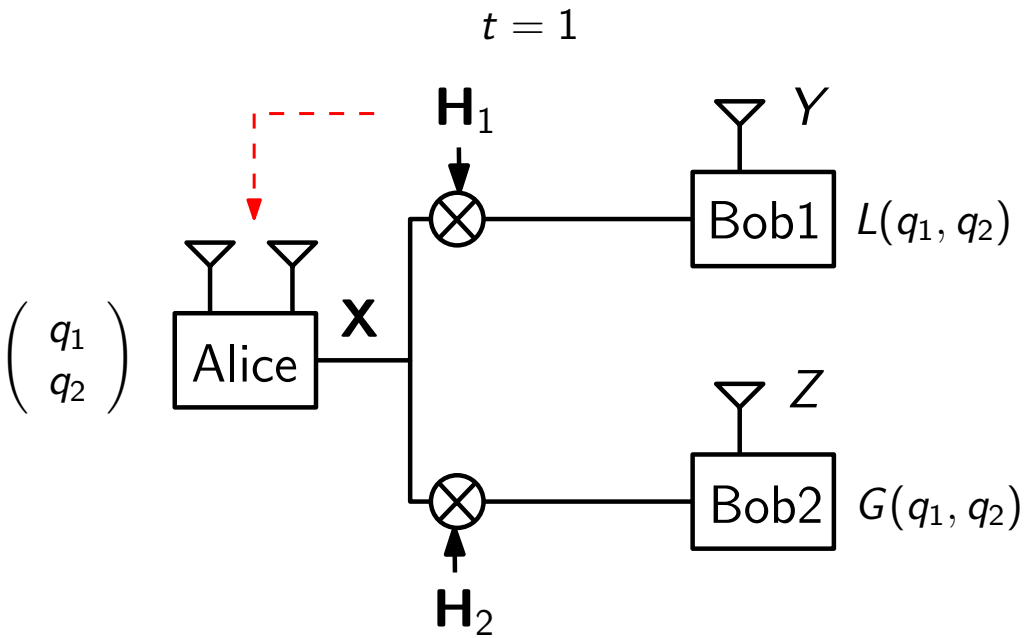
- A scheme for state PN also suffices for state PD.
- **Schemes for state PN**: Achieve s.d.o.f. pairs $(0, 1)$ and $(1, 0)$:



- The full region is achieved by time-sharing between these points.

Achievable Schemes (Contd.)

- **Schemes for state DN**: Achieve s.d.o.f. pairs $(\frac{1}{2}, 0)$ and $(0, \frac{1}{2})$:
- Achieving $(\frac{1}{2}, 0)$: Send u to first receiver in 2 time slots[a].

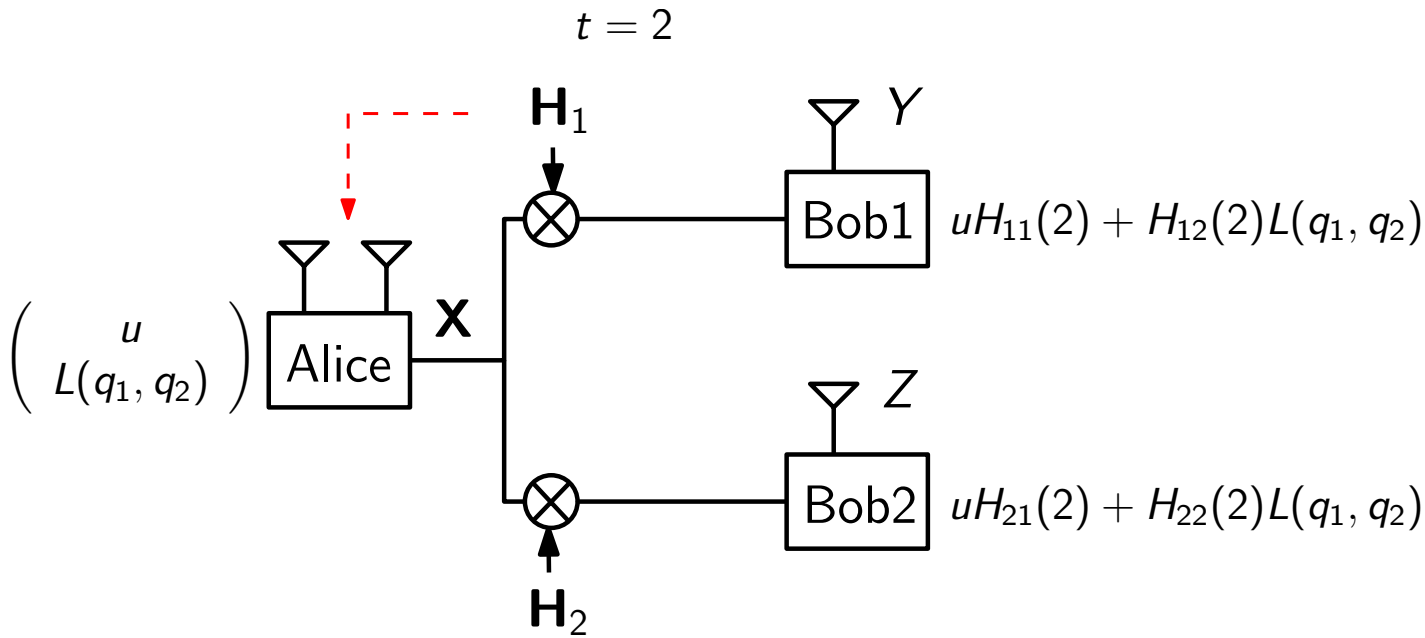


	$t = 1$	$t = 2$
Y	$L(q_1, q_2)$	
Z	$G(q_1, q_2)$	

[a] Yang et al (2013)

Achievable Schemes (Contd.)

- **Schemes for state DN**: Achieve s.d.o.f. pairs $(\frac{1}{2}, 0)$ and $(0, \frac{1}{2})$:
- Achieving $(\frac{1}{2}, 0)$: Send u to first receiver in 2 time slots[a].

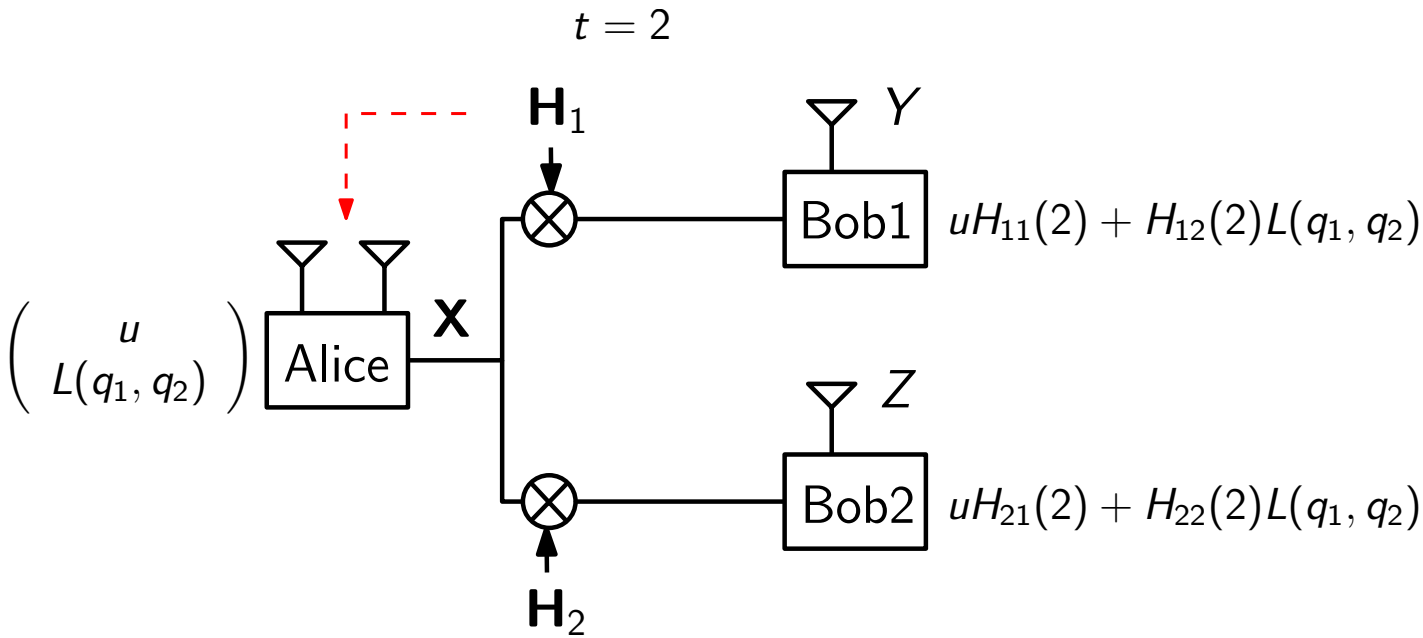


	$t = 1$	$t = 2$
Y	$L(q_1, q_2)$	$uH_{11}(2) + H_{12}(2)L(q_1, q_2)$
Z	$G(q_1, q_2)$	$uH_{21}(2) + H_{22}(2)L(q_1, q_2)$

[a] Yang et al (2013)

Achievable Schemes (Contd.)

- **Schemes for state DN**: Achieve s.d.o.f. pairs $(\frac{1}{2}, 0)$ and $(0, \frac{1}{2})$:
- Achieving $(\frac{1}{2}, 0)$: Send u to first receiver in 2 time slots[a].

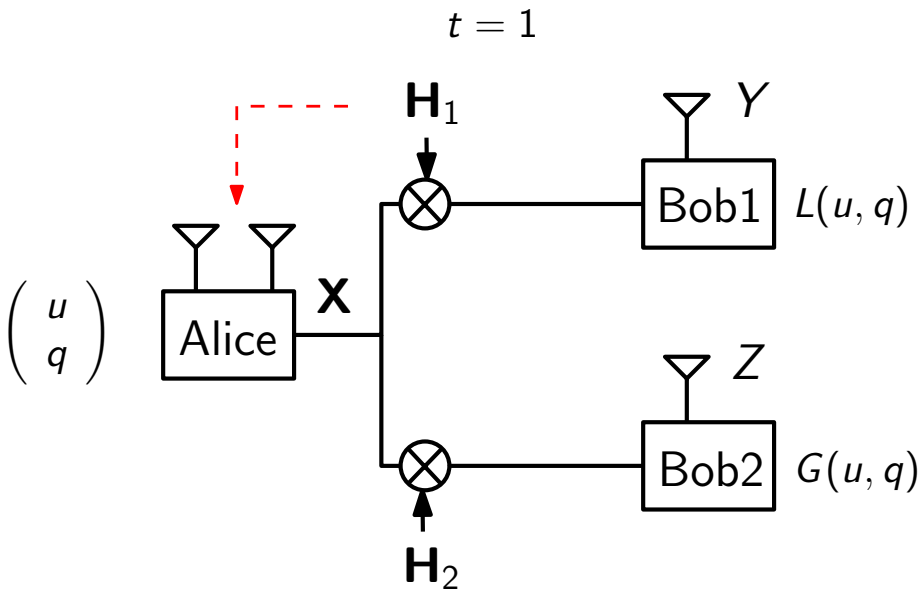


	$t = 1$	$t = 2$
Y	$L(q_1, q_2)$	$uH_{11}(2) + H_{12}(2)L(q_1, q_2)$
Z	$G(q_1, q_2)$	$uH_{21}(2) + H_{22}(2)L(q_1, q_2)$

[a] Yang et al (2013)

Achievable Schemes (Contd.)

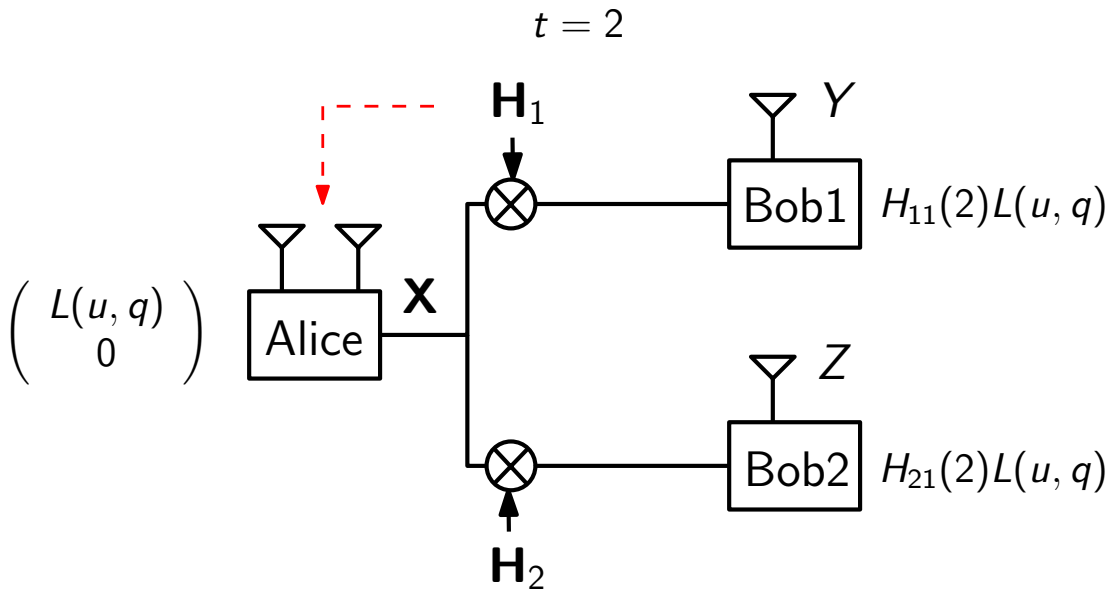
- Achieving $(0, \frac{1}{2})$: Send u to second receiver in 2 time slots.



	$t = 1$	$t = 2$
Y	$L(u, q)$	
Z	$G(u, q)$	

Achievable Schemes (Contd.)

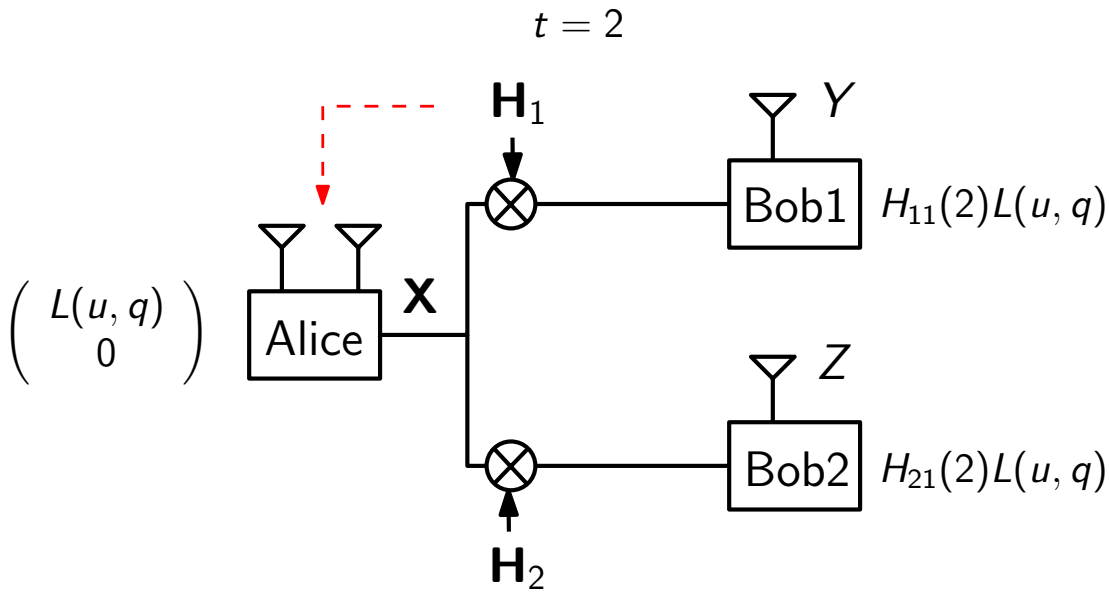
- Achieving $(0, \frac{1}{2})$: Send u to second receiver in 2 time slots.



	$t = 1$	$t = 2$
Y	$L(u,q)$	$H_{11}(2)L(u,q)$
Z	$G(u,q)$	$H_{21}(2)L(u,q)$

Achievable Schemes (Contd.)

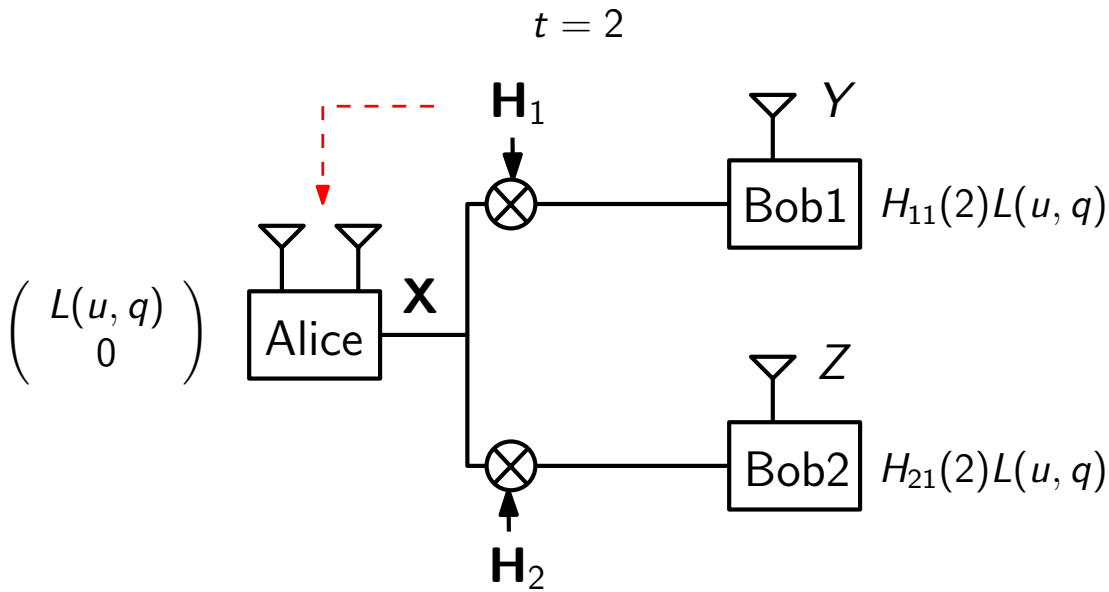
- Achieving $(0, \frac{1}{2})$: Send u to second receiver in 2 time slots.



	$t = 1$	$t = 2$
Y	$L(u,q)$	$H_{11}(2)L(u,q)$
Z	$G(u,q)$	$H_{21}(2)L(u,q)$

Achievable Schemes (Contd.)

- Achieving $(0, \frac{1}{2})$: Send u to second receiver in 2 time slots.

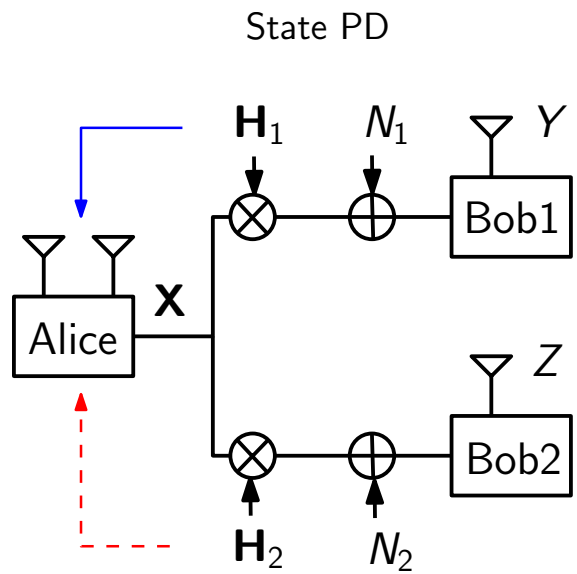


	$t = 1$	$t = 2$
Y	$L(u,q)$	$H_{11}(2)L(u,q)$
Z	$G(u,q)$	$H_{21}(2)L(u,q)$

- The full region is achieved by time-sharing between $(\frac{1}{2}, 0)$ and $(0, \frac{1}{2})$.

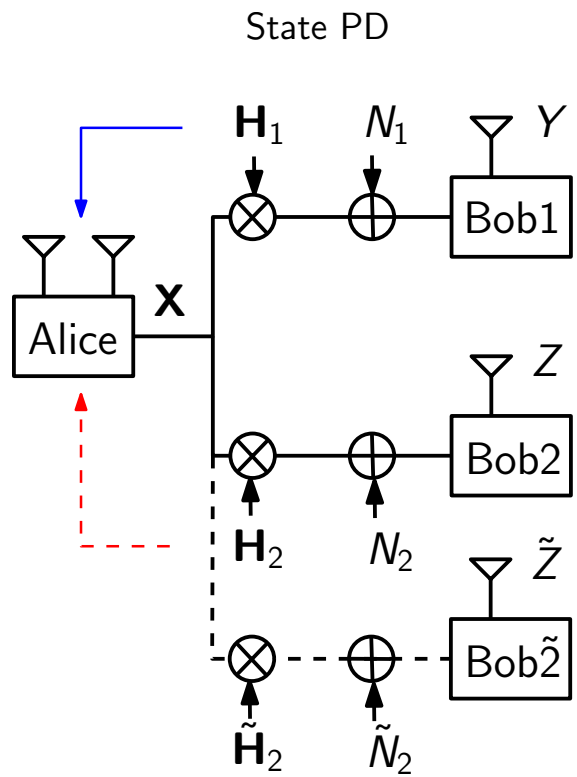
Converse Proofs

- **Key ingredient**: Local statistical equivalence.
- Consider an additional virtual output at the user supplying delayed or **no** CSIT:



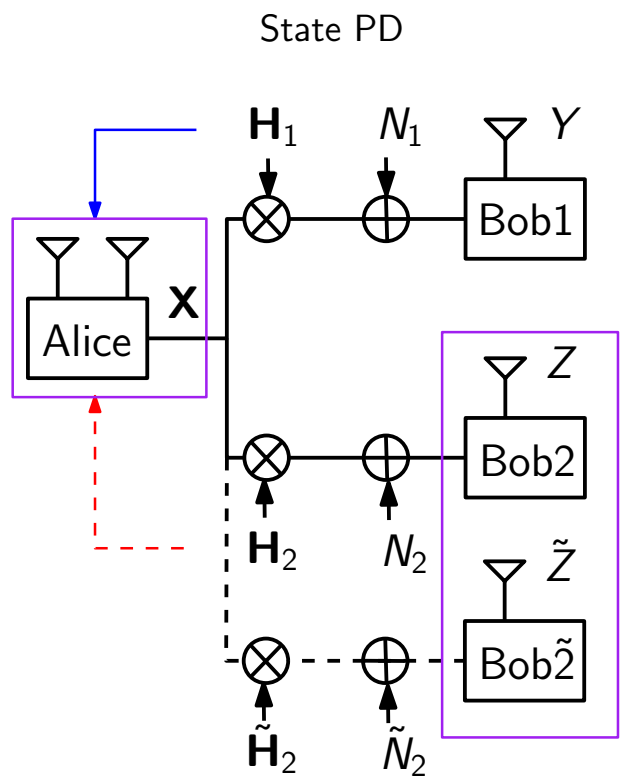
Converse Proofs

- **Key ingredient**: Local statistical equivalence.
- Consider an additional virtual output at the user supplying delayed or **no** CSIT:
- $h(Z(t)|Z^{t-1},\Omega) = h(\tilde{Z}(t)|Z^{t-1},\Omega)$.



Converse Proofs

- **Key ingredient**: Local statistical equivalence.
- Consider an additional virtual output at the user supplying delayed or **no** CSIT:
- $h(Z(t)|Z^{t-1},\Omega) = h(\tilde{Z}(t)|Z^{t-1},\Omega)$.
- Using $Z(t)$ and $\tilde{Z}(t)$, $\mathbf{X}$ can be reconstructed.

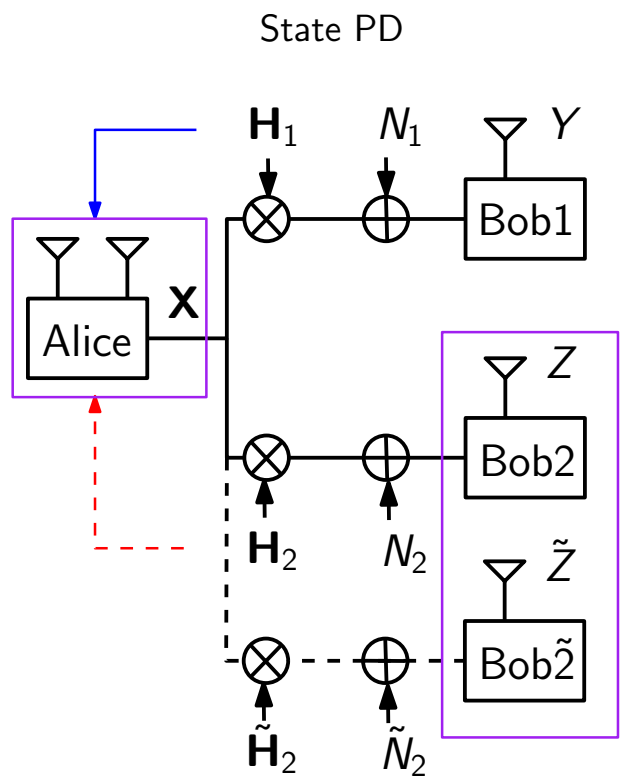


Converse Proofs

- **Key ingredient**: Local statistical equivalence.
- Consider an additional virtual output at the user supplying delayed or **no** CSIT:
- $h(Z(t)|Z^{t-1},\Omega) = h(\tilde{Z}(t)|Z^{t-1},\Omega)$.
- Using $Z(t)$ and $\tilde{Z}(t)$, $\mathbf{X}$ can be reconstructed.
- We have the following lemma:

Lemma (SEP)

$$h(Z^n|\Omega) \geq h(Y^n|Z^n,\Omega)$$
$$2h(Z^n|\Omega) \geq h(Y^n|\Omega)$$



Converse Proofs (Contd.)

Converse for states PD and PN

- Converse for state PD suffices as a converse for state PN.
- For the first user:

$$\begin{aligned} nR_1 &\leq I(W_1; Y^n|W_2) - I(W_1; Z^n|W_2) \\ &\leq I(W_1; Y^n|Z^n, W_2) \\ &\leq h(Y^n|Z^n, W_2) \\ &\overset{SEP}{\leq} h(Z^n|W_2) \end{aligned}$$

- For the second user:

$$nR_2 \leq n \log P - h(Z^n|W_2)$$

- Thus, eliminating $h(Z^n|W_2)$, and taking limits,

$$d_1 + d_2 \leq 1$$

Converse Proofs (Contd.)

Converse for state DN

- For the first user:

$$\begin{aligned} nR_1 &\leq I(W_1; Y^n) - I(W_1; Z^n) \\ &= h(Y^n) - h(Y^n|W_1) - h(Z^n) + h(Z^n|W_1) \\ &\overset{SEP}{\leq} h(Y^n) - \frac{1}{2}h(Z^n|W_1) - h(Z^n) + h(Z^n|W_1) \\ &= h(Y^n) + \frac{1}{2}h(Z^n|W_1) - h(Z^n) \\ &\leq h(Y^n) - \frac{1}{2}h(Z^n) \end{aligned} \tag{1}$$

- For the second user:

$$\begin{aligned} nR_2 \leq & I(W_2; Z^n) - I(W_2; Y^n) \\ = & h(Z^n) - h(Y^n) + (h(Y^n|W_2) - h(Z^n|W_2)) \end{aligned} \tag{2}$$

- Adding (1) and (2), we have

$$n(R_1 + R_2) \leq \frac{1}{2}h(Z^n) + (h(Y^n|W_2) - h(Z^n|W_2))$$

Converse Proofs (Contd.)

Converse for state DN

- To upper bound $(h(Y^n|W_2) - h(Z^n|W_2))$:
- **Enhance** the state DN to state PN and drop security constraints.
- For the enhanced state PN with no security constraints[a]

$$h(Y^n|W_2) - h(Z^n|W_2) \leq n\, o(\log P)$$

- Thus, we have,

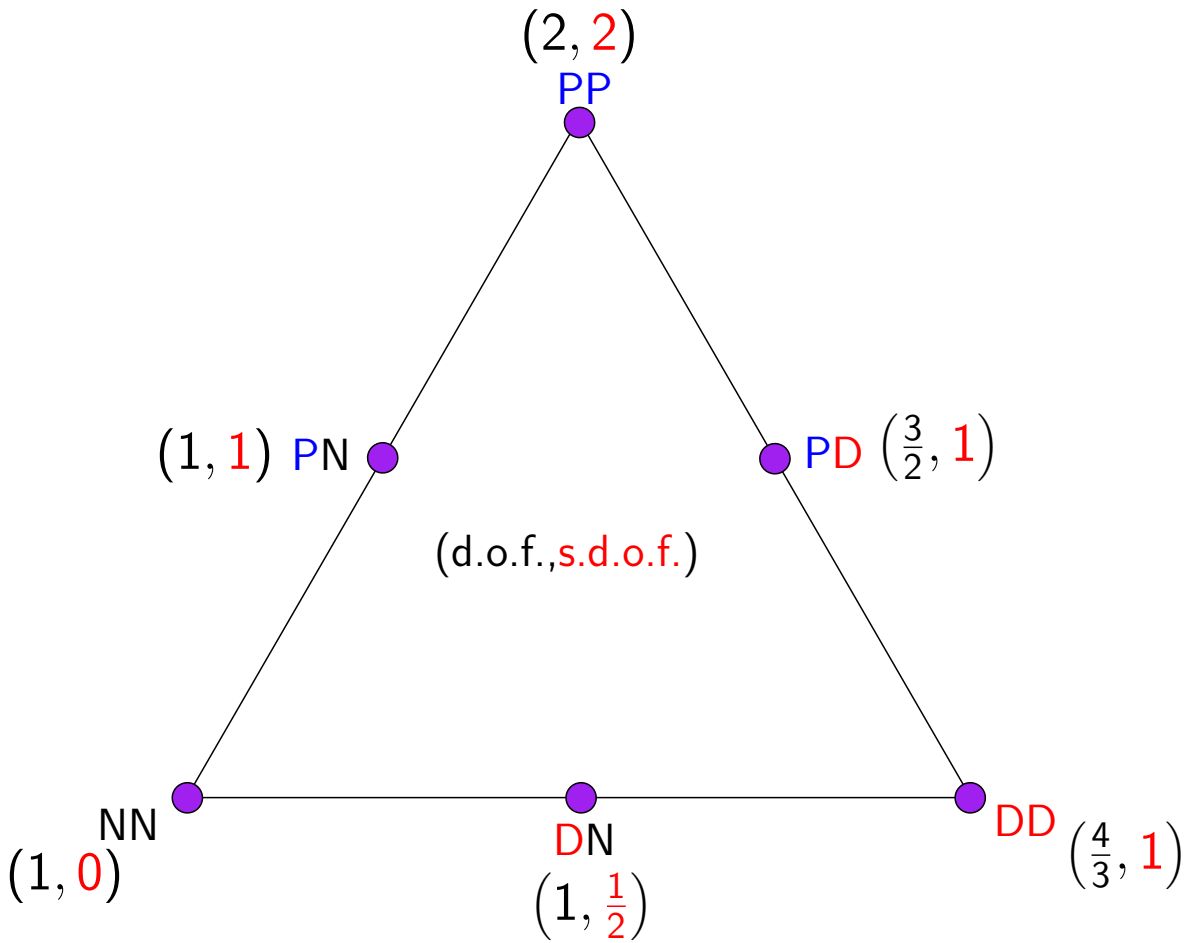
$$n(R_1 + R_2) \leq \frac{1}{2} h(Z^n) + n\, o(\log P)$$

- Using $h(Z^n) \leq n \log P$ and taking limits,

$$d_1 + d_2 \leq \frac{1}{2}$$

[a] Davoodi, Jafar (2014)

Summary



Conclusions

- Studied the MISO BCCM with heterogeneous CSIT.
- Established the full s.d.o.f. region for all three heterogeneous states.
- Achievable schemes using artificial noise and alignment techniques.
- Converses using the *local statistical equivalence* property.