The Secrecy Capacity of The Gaussian Wiretap Channel with Rate-Limited Help at the Encoder

Sergey Loyka, Neri Merhav

University of Ottawa, Technion
sergey.loyka@uottawa.ca, merhav@ee.technion.ac.il

2023 IEEE Information Theory Workshop (ITW 2023)
Saint-Malo, France, 23 - 28 April 2023 (in-person)

Introduction

- Physical layer security[1]
- Wiretap channels[2] (WTC)
  - keep Ev ignorant of Tx message
  - widely-used model
  - key metric: secrecy capacity
  - well-known in many cases
  - including feedback, jamming

[1] C. E. Shannon, Communication Theory of Secrecy Systems, Bell Syst. Tech. J., Oct. 1949.

[2] A.D. Wyner, The Wire-Tap Channel, Bell Syst. Tech. J., Oct. 1975.

Introduction: Is Feedback Useful?

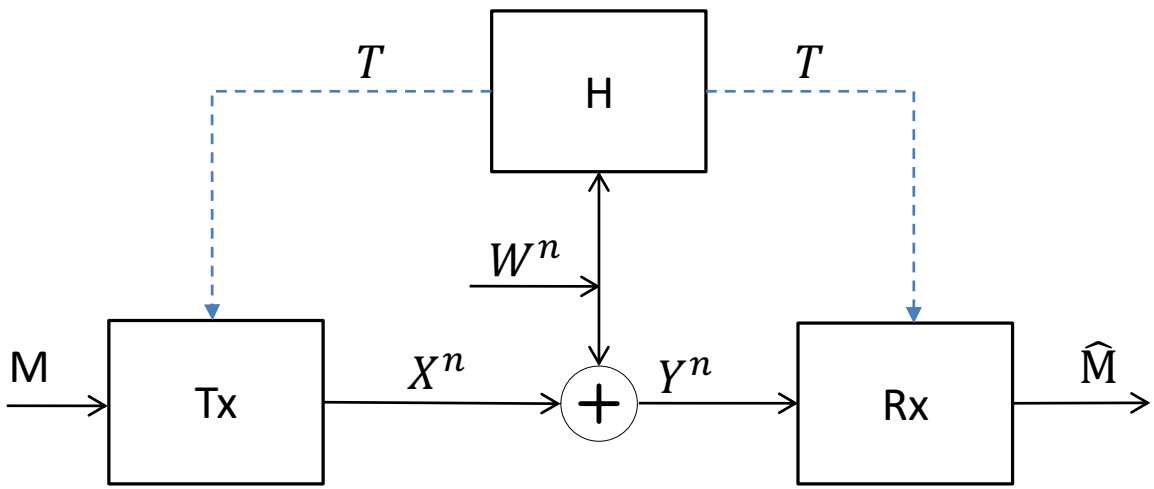
- No boost for regular (no secrecy) capacity of memoryless channels
- **But...** boosts secrecy capacity, even if memoryless!
- **However...**
- Unrealistic assumptions
  - noiseless FB link (infinite capacity)
    - arbitrarily-low noise destroys achievability
  - perfect secrecy of FB link

This Paper

- More realistic assumtions
- Rate-limited help at the Tx
  - Secure and non-secure
  - Causal and non-causal
- Boosts secrecy capacity
- **...even if not secure...**
- "Free-lunch" theorem

New twist: help instead of feedback (no Ev yet)

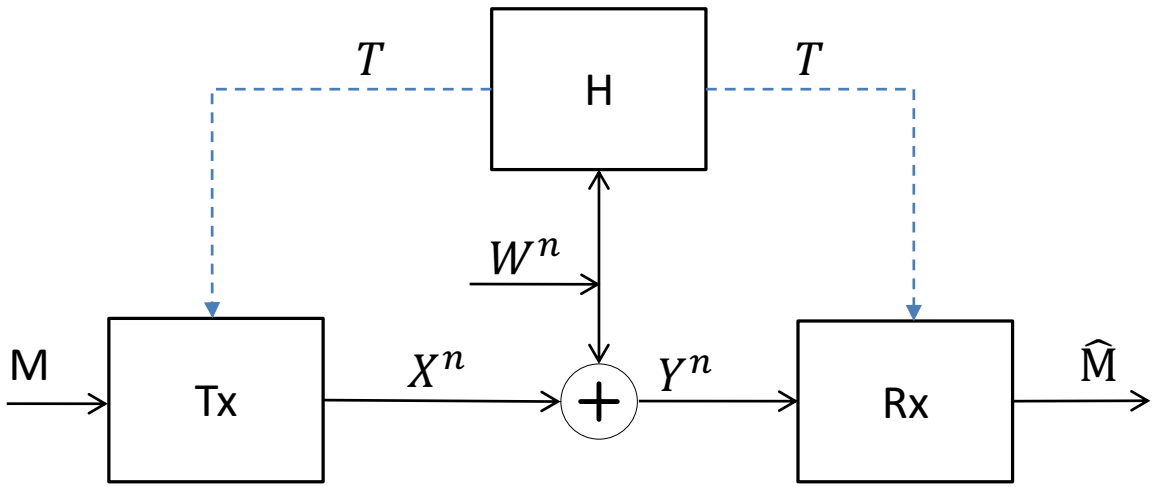
- additive-noise channels
- helper: observes noise sequence
- rate-limited (!) help[3][4] instead of noiseless (infinite-rate) feedback



[3] S. I. Bross, A. Lapidoth, G. Marti, Decoder-assisted communications over additive noise channels, IEEE Trans. Commun., Jul. 2020.

[4] A. Lapidoth, G. Marti, Encoder-Assisted Communications Over Additive Noise Channels, IEEE Trans. Info. Theory, Nov. 2020.

New twist: help instead of feedback (no Ev yet)



the capacity: $+R_h$ rate boost

$$C = C_0 + R_h \tag{1}$$

optimal signaling: 2-phase flash signaling

New twist: help instead of feedback (no Ev yet)

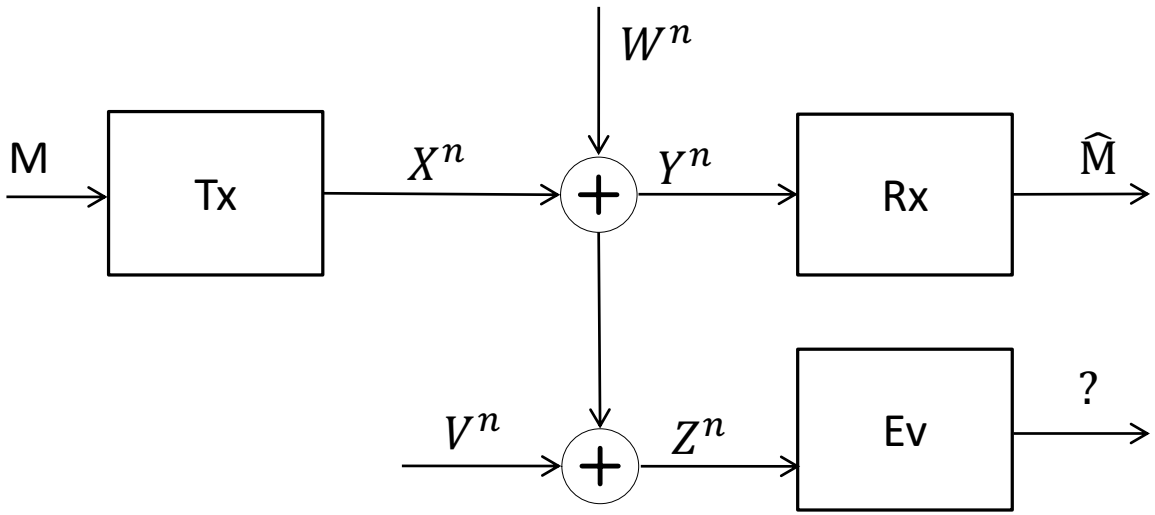
- key advantage: no infinite-capacity (noiseless) feedback links
- applications
  - cloud radio access
  - cellular
  - WiFi

This work: WTC + Help

- additive-noise WTC + Tx/Rx help (no jamming)
  - degraded
  - reversely-degraded
  - non-degraded
- help: rate-limited, secure or not, causal or not
- $+R_h$ boost in secrecy rates, even if
  - help is not secure
  - channel is reversely degraded
  - help is causal
- "free lunch" theorem

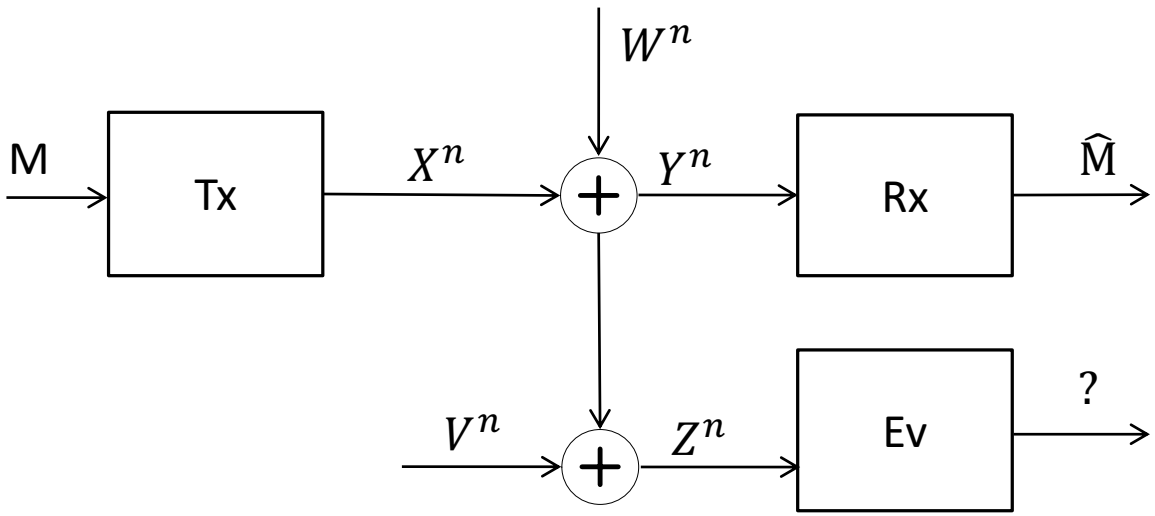
Degraded Wiretap Channel (no help yet)

- $M \to X^n \to Y^n \to Z^n$
- additive noise: $Y_i = X_i + W_i,\ Z_i = Y_i + V_i$



- weak secrecy (Ev): $R_l = n^{-1} I(M; Z^n) \leq \epsilon$
- reliability (Rx): $\Pr\{M \neq \hat{M}\} \leq \varepsilon$
- power (Tx): $\frac{1}{n} \sum_{i=1}^{n} \mathbb{E}|X_i|^2 \leq P$

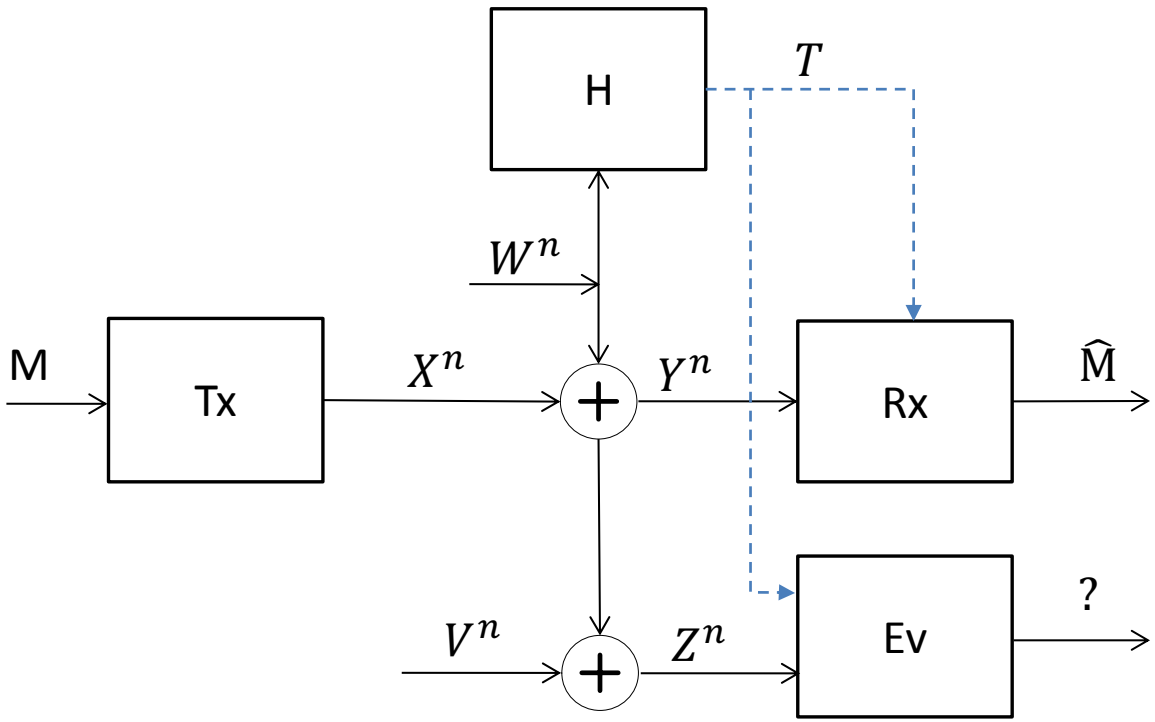
Degraded Wiretap AWGN Channel



- secrecy capacity: $C_{s0} = C_1 - C_2 = \log \frac{1+\gamma_1}{1+\gamma_2}$
- C_1, C_2: Tx-Rx and Tx-Ev capacities

Degraded Wiretap Channel with Rx Help[5]

- ... and **rate-limited** Rx help: $n^{-1}H(T) \leq R_h$
- Rx decoding: based on Y^n and T
- Ev: arbitrary-low leakage rate $R_l = n^{-1}I(M; Z^n T) \leq \epsilon$



[5] S. Loyka, N. Merhav, The Secrecy Capacity of Gaussian Wiretap Channels with Rate-Limited Help at the Decoder, ISIT 2022.

Degraded Wiretap Channel with Rx Help[7]

- secrecy capacity:

$$C_s = C_{s0} + R_h \tag{2}$$

- i.e. $+R_h$ boost due to help
- the same as in the no-secrecy case[6]
- i.e. the boost comes with secrecy **for free**
- extends to reversely-degraded case, where $C_{s0} = 0$ (no help), even if help is not secure:

$$C_s = R_h \tag{3}$$

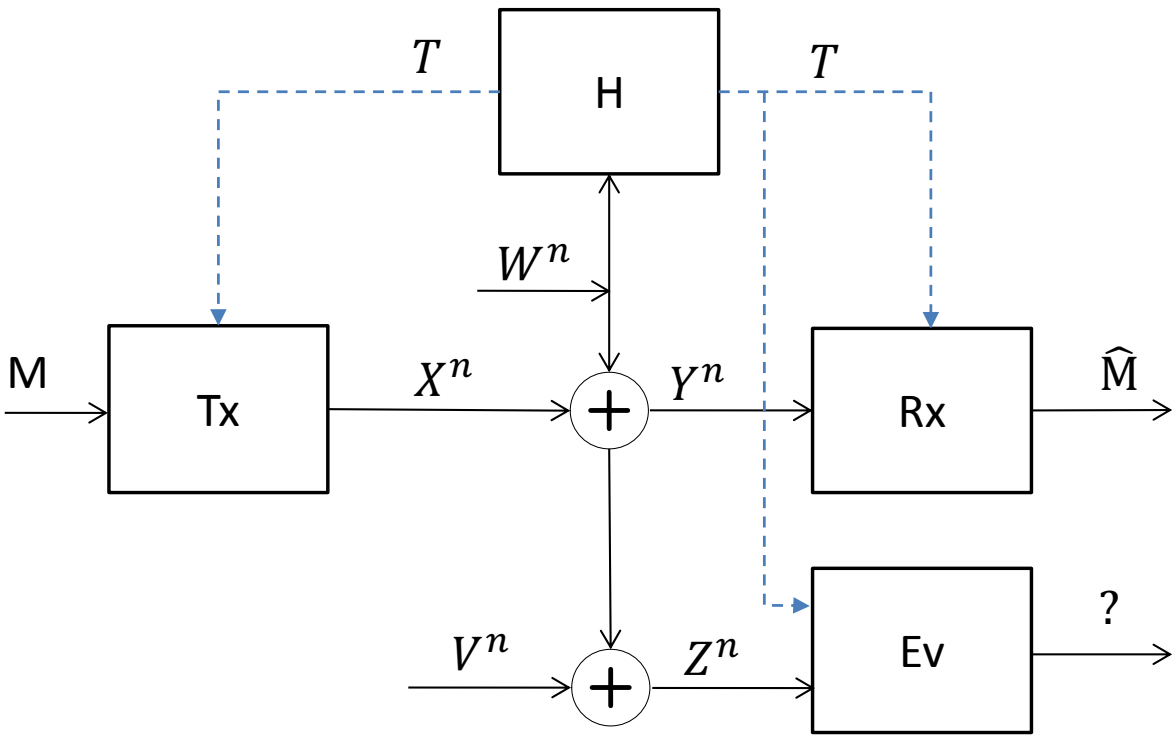
- no wiretap coding is needed to achieve it

[6] S. I. Bross, A. Lapidoth, G. Marti, Decoder-assisted communications over additive noise channels, IEEE Trans. Commun., Jul. 2020.

[7] S. Loyka, N. Merhav, The Secrecy Capacity of Gaussian Wiretap Channels with Rate-Limited Help at the Decoder, ISIT 2022.

This Paper: Tx Help

- in addition to or instead of Rx help
- secure or not
- causal or not



This Paper: Tx Help

- degraded Gaussian WTC
- Tx or/and Rx help of rate R_h
- causal or not
- secure or not

Theorem

Lower bound on secrecy capacity C_s:

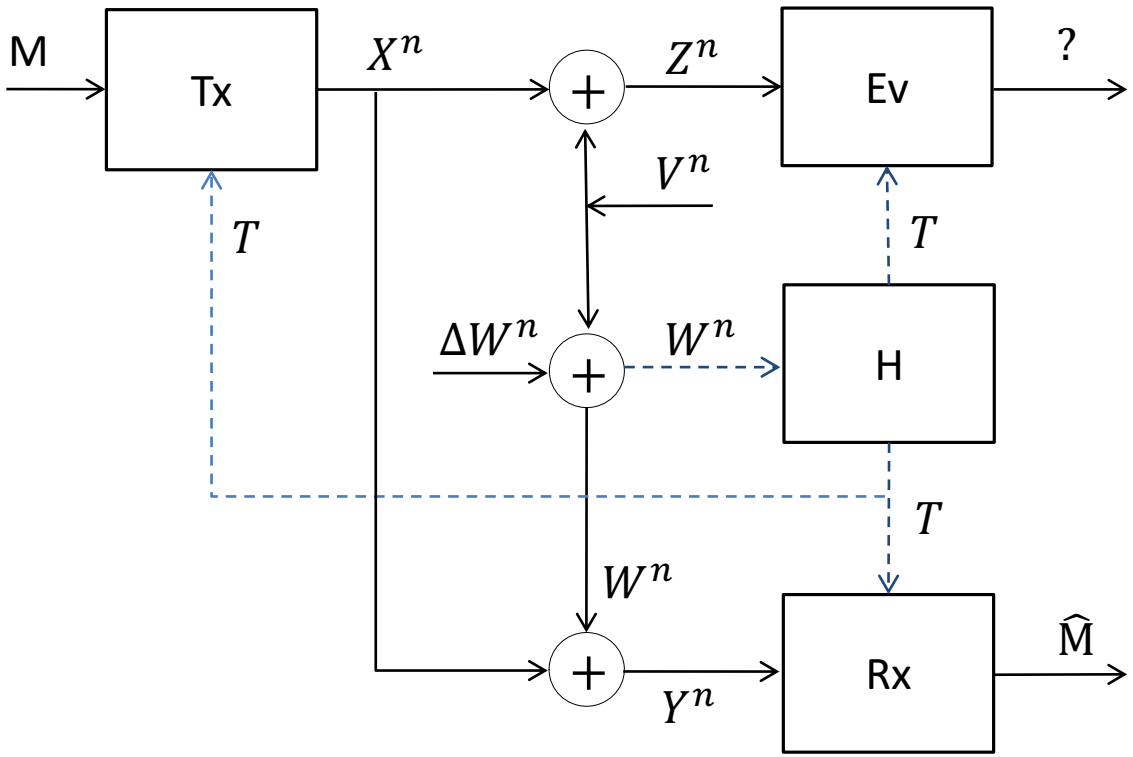
$$C_s \geq C_{s0} + R_h \tag{4}$$

Holds with equality if help is not secure.

- same Rx help, in addition to Tx help: no extra boost in C_s
- non-causal Tx help: no extra boost over the causal one

Reversely-Degraded Wiretap Channel

- $M \to X^n \to Z^n \to Y^n$



- No help: $C_{s0} = 0$ (no secrecy)

Reversely-Degraded Gaussian WTC

- no-help secrecy capacity $C_{s0} = 0$
- ...but not so with help

Theorem

Lower bound on secrecy capacity C_s:

$$C_s \geq R_h \tag{5}$$

Holds with equality if help is not secure.

- positive secrecy rates, ... even if help is not secure

Reversely-Degraded Gaussian WTC

Theorem

Lower bound on secrecy capacity C_s:

$$C_s \geq R_h \tag{6}$$

Holds with equality if help is not secure.

- extra noise at Rx $\rightarrow$ higher sec. capacity !
- $C_s > 0$ is possible, even if help is not secure!
- **but why?**
  - Rx is degraded w.r.t. Ev
  - help is not secure
  - if Rx recovers secret message $\rightarrow$ so does Ev ?!

but why?

- slight difference in noise can be exploited
- even if Rx noise $>$ Ev noise
- even if help is not secure
  - $T = Q(W^n) =$ public key
  - only Rx has the exact lock ($Z^n \neq W^n$)

Reversely Degraded Wiretap Channel + Tx Help

Achievability:

- burst signaling, phase 2 only (no phase 1)
- no wiretap coding at all !
- burst transmission $\rightarrow$ secrecy
- well-known in the spying world[8] :)

[8] E. Shannon, Death of The Perfect Spy, Time, June 24, 2001.

Reversely Degraded Wiretap Channel + Tx Help

Achievability:

- burst signaling, phase 2 only (no phase 1)
- no wiretap coding at all !
- burst transmission $\rightarrow$ secrecy
- well-known in the spying world[8] :)

[8] E. Shannon, Death of The Perfect Spy, Time, June 24, 2001.

Conclusion

- Wiretap channel + Tx help of rate R_h
- $+R_h$ boost in secrecy rates, even if help is not secure
  - degraded
  - reversely-degraded ($C_s > 0$)
  - non-degraded
- **open problem**: secure Tx help, non-degraded WTC

"free lunch" theorem:

- Rx/Tx help: $+R_h$ boost comes with secrecy for free

Conclusion

- Wiretap channel + Tx help of rate R_h
- $+R_h$ boost in secrecy rates, even if help is not secure
  - degraded
  - reversely-degraded ($C_s > 0$)
  - non-degraded
- **open problem**: secure Tx help, non-degraded WTC

"free lunch" theorem:

- Rx/Tx help: $+R_h$ boost comes with secrecy for free

Role of Feedback (FB)

- Memoryless channels (e.g. AWGN): no impact on capacity C_0
- WTC: FB boosts secrecy capacity C_s in many cases
- AWGN WTC, noseless FB to Tx but noisy to Ev[9]

$$C_s = C_0 > C_{s0} \tag{7}$$

  i.e. secrecy comes for free!

- Extended to colored (ARMA) noise[10]
- **But...**
  - noisy FB to Ev, i.e. (partially) secret FB
  - noiseless FB to Tx: rate-unlimited (impossible in practice)

[9] D. Gunduz et al, Secret Communication With Feedback, Dec. 2008.

[10] C. Li at al, Secrecy Capacity of Colored Gaussian Noise Channels With Feedback, IEEE Trans. Info. Theory, Sep. 2019.

Role of Feedback (FB)

- Memoryless channels (e.g. AWGN): no impact on capacity C_0
- WTC: FB boosts secrecy capacity C_s in many cases
- AWGN WTC, noseless FB to Tx but noisy to Ev[9]

$$C_s = C_0 > C_{s0} \tag{7}$$

  i.e. secrecy comes for free!

- Extended to colored (ARMA) noise[10]
- **But...**
  - noisy FB to Ev, i.e. (partially) secret FB
  - noiseless FB to Tx: rate-unlimited (impossible in practice)

[9] D. Gunduz et al, Secret Communication With Feedback, Dec. 2008.

[10] C. Li at al, Secrecy Capacity of Colored Gaussian Noise Channels With Feedback, IEEE Trans. Info. Theory, Sep. 2019.

Role of Feedback (FB)

- Memoryless channels (e.g. AWGN): no impact on capacity C_0
- WTC: FB boosts secrecy capacity C_s in many cases
- AWGN WTC, noseless FB to Tx but noisy to Ev[9]

$$C_s = C_0 > C_{s0} \tag{7}$$

  i.e. secrecy comes for free!

- Extended to colored (ARMA) noise[10]
- **But...**
  - noisy FB to Ev, i.e. (partially) secret FB
  - noiseless FB to Tx: rate-unlimited (impossible in practice)

[9] D. Gunduz et al, Secret Communication With Feedback, Dec. 2008.

[10] C. Li at al, Secrecy Capacity of Colored Gaussian Noise Channels With Feedback, IEEE Trans. Info. Theory, Sep. 2019.

Role of Feedback (FB)

- *Rate-limited* secure FB[11]

$$C_{sf} = \min\{C_0, C_{s0} + R_f\} \tag{8}$$

- **But...**
  - secure FB to Tx
  - does not work if non-secure FB

[11] E. Ardestanizadeh et al, Wiretap Channel With Secure Rate-Limited Feedback, IEEE Trans. Info. Theory, Dec. 2009.