# Full-duplex vs. Half-duplex secret-key generation

Hendrik Vogt, Aydin Sezgin

WIFS 2015
Rome, Italy

Lehrstuhl für
**Digitale**
**Kommunikationssysteme**

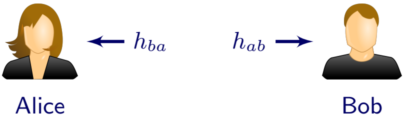
Fakultät für
Elektrotechnik und
Informationstechnik

# Contents

# Contents

# Classic secret-key generation

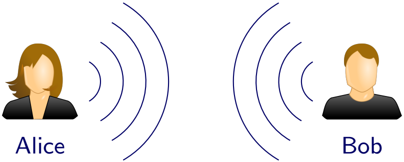
Basic idea: Utilize reciprocal channel states as shared secret




1. Channel estimation by **half-duplex (HD)** probing

# Classic secret-key generation

Basic idea: Utilize reciprocal channel states as shared secret




1. Channel estimation by **half-duplex (HD)** probing
2. Alice and Bob "talk" about their estimations by **HD** communication (key reconciliation)

# Classic secret-key generation

Basic idea: Utilize reciprocal channel states as shared secret


1. Channel estimation by **half-duplex (HD)** probing
2. Alice and Bob "talk" about their estimations by **HD** communication (key reconciliation)
3. Reduce leakage to eavesdropper (privacy amplification)

# Classic secret-key generation

Basic idea: Utilize reciprocal channel states as shared secret


1. Channel estimation by **half-duplex (HD)** probing
2. Alice and Bob "talk" about their estimations by **HD** communication (key reconciliation)
3. Reduce leakage to eavesdropper (privacy amplification)
4. Bit strings are declared as secret key

# In-band full-duplex (IBFD)


- IBFD means transmitting/receiving at the **same** time and frequency band
- Key technology in 5G
- Self-interference problem is challenging, but manageable (successful **prototypes**!)

# In-band full-duplex (IBFD)


- IBFD means transmitting/receiving at the **same** time and frequency band
- Key technology in 5G
- Self-interference problem is challenging, but manageable (successful **prototypes**!)

**Key advantage**

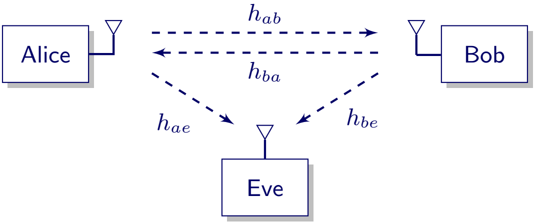
Simultaneous channel probing is **downgrading** an eavesdropper!

# Proposed secret-key generation


1. Channel estimation by **full-duplex (FD)** probing
2. Alice and Bob "talk" about their estimations by **FD** communication (key reconciliation)
3. . . .
4. . . .

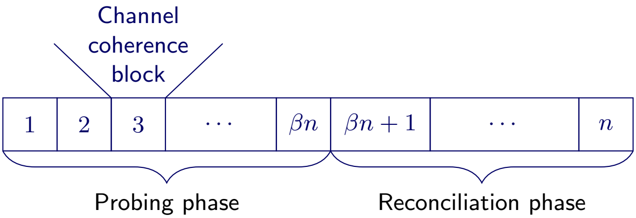
# Contents

# Nodes in scene




- **Single**-antenna scenario, multi-antenna Eve emulated by higher correlation
- Channels comply with **real**-valued **flat**-fading model
- Alice and Bob can switch between **HD** and **FD** mode

# Execution flow




**Probing phase** Obtain channel estimations by probing

**Reconciliation phase** Alice transmits message to Bob

**Key generation** Based on estimations and reconciliation, Alice and Bob agree on a key

# Probing phase (HD mode)

| | |
|---|---|
| **Alice** | $x = \sqrt{\mathrm{snr}}\, h_{ba} + n_a$ |
| **Bob** | $y = \sqrt{\mathrm{snr}}\, h_{ab} + n_b$ |
| **Eve** | $z_1 = \sqrt{\mathrm{snr}_{\mathrm{ae}}}\, h_{ae} + n_{ae}$ <br> $z_2 = \sqrt{\mathrm{snr}_{\mathrm{be}}}\, h_{be} + n_{be}$ |

- Channels $h_{ij}$ are jointly **Gaussian** distributed with zero mean and unit variance
- Correlation measure $\mathbb{E}\left[h_{ba} h_{ab}\right] = \delta \cdot \rho_{ba}$
- Parameter $0 < \delta < 1$ denotes the **penalty** of delayed HD probing

# Probing phase (FD mode)

| | |
|---|---|
| **Alice** | $x = \sqrt{\mathrm{snr}}\, h_{ba} + \alpha \sqrt{\mathrm{snr}}\, n_{\mathsf{l}a} + n_a$ |
| **Bob** | $y = \sqrt{\mathrm{snr}}\, h_{ab} + \alpha \sqrt{\mathrm{snr}}\, n_{\mathsf{l}b} + n_b$ |
| **Eve** | $z = \sqrt{\mathrm{snr}_{\mathrm{ae}}}\, h_{ae} + \sqrt{\mathrm{snr}_{\mathrm{be}}}\, h_{be} + n_e$ |

- Alice and Bob suffer from Gaussian self-interference (SI)
- Parameter $0 < \alpha < 1$ denotes the strength of **residual** SI
- Eve obtains only a **superposition** of probing signals

# Reconciliation phase


- Alice sends an authenticated, public message to Bob
- This is *point-to-point* communication over a fading channel
- Bob has only **partial** channel state information

**Communication rate $R_p$**

Number of bits per channel use that satisfy **reliability** condition

# Contents

# Rates

## Secret-key rate $R_{sk}$

Number of bits per channel estimation that satisfy

1. Reliability
2. Uniformity
3. Secrecy

conditions.

- Functional relationship between $R_{sk}$ and communication rate $R_p$: Key-communication function

# Key-communication function

$$R_{sk}(R_p) = \frac{\beta}{2} \log_2 \frac{1 - 2^{-2\frac{R_p}{\beta}} (\|\boldsymbol{b}_x\|^2 - \|\boldsymbol{e}_x\|^2) + \|\boldsymbol{b}_x\|^2}{1 + \|\boldsymbol{e}_x\|^2}$$

| | |
|---|---|
| $\beta$ | **Time-sharing** of probing and reconciliation phase |
| $R_p$ | Communication rate during reconciliation phase |
| $\|\boldsymbol{b}_x\|^2$ | Quality of **legitimate users'** estimation |
| $\|\boldsymbol{e}_x\|^2$ | Quality of **Eve's** estimation |

# Key-communication function

$$R_{sk}(R_p) = \frac{\beta}{2} \log_2 \frac{1 - 2^{-2\frac{R_p}{\beta}} (\|\boldsymbol{b}_x\|^2 - \|\boldsymbol{e}_x\|^2) + \|\boldsymbol{b}_x\|^2}{1 + \|\boldsymbol{e}_x\|^2}$$

## Property

$R_{sk}$ is **positive** if and only if

1. $R_p > 0$,
2. $\|\boldsymbol{b}_x\|^2 > \|\boldsymbol{e}_x\|^2$

hold.

## Key-communication function

$$R_{sk}(R_p) = \frac{\beta}{2} \log_2 \frac{1 - 2^{-2\frac{R_p}{\beta}} (\|\boldsymbol{b}_x\|^2 - \|\boldsymbol{e}_x\|^2) + \|\boldsymbol{b}_x\|^2}{1 + \|\boldsymbol{e}_x\|^2}$$

- We apply the key-communication function to **HD** and **FD** modes
- HD mode - Upper bound

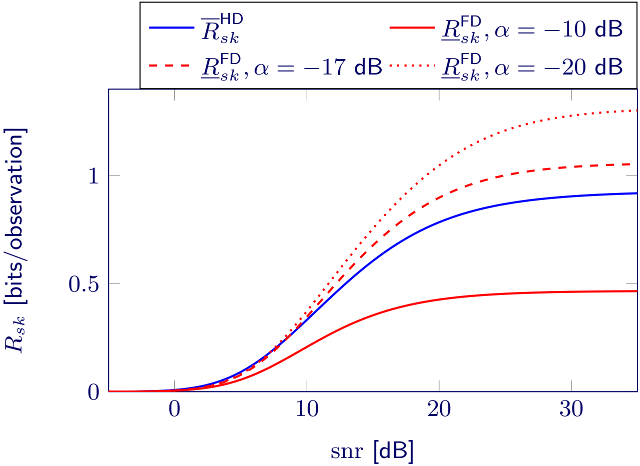
$$R_{sk}^{\mathsf{HD}}(R_p^{\mathsf{HD}}) < \overline{R}_{sk}^{\mathsf{HD}}$$

- FD mode - Lower bound

$$R_{sk}^{\mathsf{FD}}(R_p^{\mathsf{FD}}) > \underline{R}_{sk}^{\mathsf{FD}}$$

# Contents

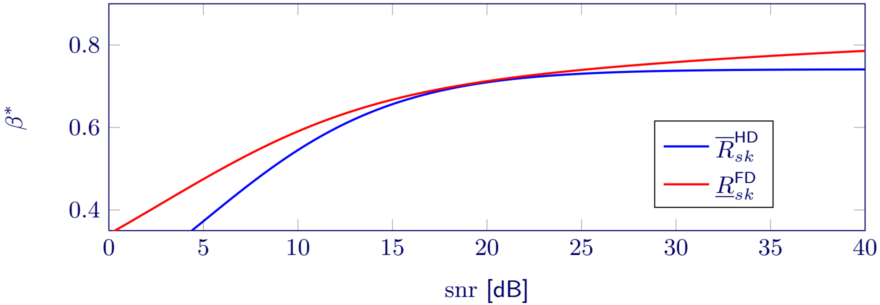
# HD vs. FD performance




- Parameters $\rho_{ae} = \rho_{be} = \rho_e = 0.4$, $\rho_{ba}^2 = 1$, $\delta = 0.97$, $\text{snr}_{\text{ae}} = \text{snr}_{\text{be}} = \text{snr}$ and $\beta = 0.5$

# Probing-reconciliation trade-off

Time-sharing $\beta$ between **probing** and **reconciliation** phase can be optimized




- Parameters: $\rho_{ba} = 1$, $\delta = 0.95$, $\rho_{ae} = \rho_{be} = \rho_e = 0.4$, $\text{snr}_{\text{ae}} = \text{snr}_{\text{be}} = \text{snr}$ and $\alpha = -15$ dB.

# Conclusion

- We formulate a system model for channel probing and reconciliation phases for **HD** and **FD** modes
- We derive the key-communication function and provide bounds for **HD** and **FD** modes
- Simulations show **FD** system often performs better than **HD**, the impact of SI is **insignificant**
- Trade-off between probing and reconciliation phase is different for **HD** and **FD** modes

Thank you! Any questions?