Key Assistance, Key Agreement, and Layered Secrecy for Bosonic Broadcast Channels

Uzi Pereg

Technical University of Munich (TUM)

Joint Work with Roberto Ferrara and Matthieu R. Bloch

ITW 2021

Motivation: Key Agreement

- Physical-layer security requires the communication of private information to be secret, regardless of computational capabilities.
    - Secret-key agreement is a promising method to achieve this goal, whereby the sender and receiver generate a secret key before communication takes place.

Motivation: Key Agreement

- Physical-layer security requires the communication of private information to be secret, regardless of computational capabilities.
  - Secret-key agreement is a promising method to achieve this goal, whereby the sender and receiver generate a secret key before communication takes place.
  - In practice, quantum key distribution (QKD) is the most mature application of quantum information theory

Motivation: Key Agreement

- Physical-layer security requires the communication of private information to be secret, regardless of computational capabilities.
  - Secret-key agreement is a promising method to achieve this goal, whereby the sender and receiver generate a secret key before communication takes place.
  - In practice, quantum key distribution (QKD) is the most mature application of quantum information theory
- In some noise models, communication can also be secured without key assistance.

Motivation: Layered Secrecy

- The Layered Secrecy model describes a network in which multiple users have different credentials to access confidential information.
- For example: a WiFi network of an agency, in which a user is allowed to receive files up to a certain security clearance, but should be kept ignorant of classified files that require a higher security level [Zou et al., 2015].
    - The agency can set the channel quality on a clearance basis by assigning more communication resources to users with a higher security rank.
- In some models, this structure allows the provision of secrecy in hindsight [Tahmasbi, Bloch, and Yener, 2020].

Motivation: Layered Secrecy

- The Layered Secrecy model describes a network in which multiple users have different credentials to access confidential information.

- For example: a WiFi network of an agency, in which a user is allowed to receive files up to a certain security clearance, but should be kept ignorant of classified files that require a higher security level [Zou et al., 2015].
  - ∗ The agency can set the channel quality on a clearance basis by assigning more communication resources to users with a higher security rank.

- In some models, this structure allows the provision of secrecy in hindsight [Tahmasbi, Bloch, and Yener, 2020].

Motivation: Layered Secrecy

- The Layered Secrecy model describes a network in which multiple users have different credentials to access confidential information.

- For example: a WiFi network of an agency, in which a user is allowed to receive files up to a certain security clearance, but should be kept ignorant of classified files that require a higher security level [Zou et al., 2015].
  - The agency can set the channel quality on a clearance basis by assigning more communication resources to users with a higher security rank.

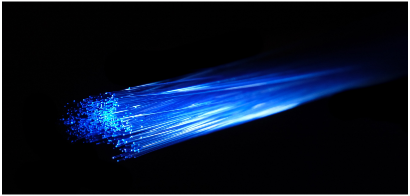
- In some models, this structure allows the provision of secrecy in hindsight [Tahmasbi, Bloch, and Yener, 2020].

Motivation: Layered Secrecy

- The Layered Secrecy model describes a network in which multiple users have different credentials to access confidential information.
- For example: a WiFi network of an agency, in which a user is allowed to receive files up to a certain security clearance, but should be kept ignorant of classified files that require a higher security level [Zou et al., 2015].
  - The agency can set the channel quality on a clearance basis by assigning more communication resources to users with a higher security rank.
- In some models, this structure allows the provision of secrecy in hindsight [Tahmasbi, Bloch, and Yener, 2020].

Motivation: Bosonic Channels

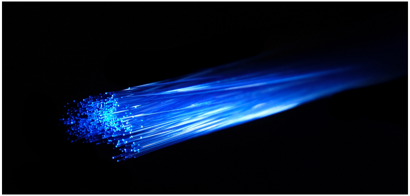
- Optical communication forms the backbone of the Internet



unsplash.com

Motivation: Bosonic Channels

- Optical communication forms the backbone of the Internet
- The bosonic (Gaussian) channel is a simple quantum-mechanical model for optical communication over free space or optical fibers



unsplash.com

Related Work

Very partial list:

Classical Security

- Secret-key agreement [Maurer, 1993] [Ahlswede and Csiszár,1993]
- Wiretap channel with key assistance [Yamamoto, 2010]
- Layered secrecy [Ly, Liu, and Blankenship, 2012] [Zou, Liang, Lai, Poor, and Shamai, 2015]

Quantum Security

- Secret-key agreement [Devetak and Winter, 2005]
- Wiretap channel [Devetak, 2005] [Cai, Winter, and Yeung, 2004]
  - key assistance [Hsieh, Luo, and Brun, 2008] [Wilde, 2011]
  - public/secret message [Hsieh and Wilde, 2009]
- Confidential Broadcast channel [Salek, Hsie, and Fonollosa, 2019]

Related Work

Very partial list:

Classical Security

- Secret-key agreement [Maurer, 1993] [Ahlswede and Csiszár,1993]
- Wiretap channel with key assistance [Yamamoto, 2010]
- Layered secrecy [Ly, Liu, and Blankenship, 2012] [Zou, Liang, Lai, Poor, and Shamai, 2015]

Quantum Security

- Secret-key agreement [Devetak and Winter, 2005]
- Wiretap channel [Devetak, 2005] [Cai, Winter, and Yeung, 2004]
  - key assistance [Hsieh, Luo, and Brun, 2008] [Wilde, 2011]
  - public/secret message [Hsieh and Wilde, 2009]
- Confidential Broadcast channel [Salek, Hsie, and Fonollosa, 2019]

Related Work (Cont.)

Bosonic broadcast channels

- Classical capacity [Guha, Shapiro, and Erkmen, 2007]
- Entanglement distillation [Takeoka, Seshadreesan, and Wilde, 2017]
- Teleportation-covariant channel [Laurenza and Pirandola, 2017]
- Amplifier channel [Qi and Wilde, 2017]
- Covertness [Anderson, Guha, and Bash, 2021]
- ...

Main Contributions

We study secret-sharing building blocks that are based on quantum broadcast communication.

- Confidential capacity region of the pure-loss bosonic broadcast channel with shared **key assistance** (under min output-entropy conjecture)

Main Contributions

We study secret-sharing building blocks that are based on quantum broadcast communication.

- Confidential capacity region of the pure-loss bosonic broadcast channel with shared **key assistance** (under min output-entropy conjecture)
- Conference **key agreement** for the distillation and distribution of joint + private keys

Main Contributions

We study secret-sharing building blocks that are based on quantum broadcast communication.

- Confidential capacity region of the pure-loss bosonic broadcast channel with shared **key assistance** (under min output-entropy conjecture)
- Conference **key agreement** for the distillation and distribution of joint + private keys
- Quantum **layered secrecy**: Three receivers with different security levels

Outline

- Key Assistance and Key Agreement
  - Definitions
  - Main Results
- Layered Secrecy
  - Channel Model
  - Main Results

Quantum Broadcast Channel

A quantum broadcast channel $\mathscr{N}_{A\to BE}$ is a linear, completely positive, trace preserving map corresponding to a quantum physical evolution:

$$\rho_A \xrightarrow{\mathscr{N}} \rho_{BE}$$

Quantum Broadcast Channel

A quantum broadcast channel $\mathscr{N}_{A\to BE}$ is a linear, completely positive, trace preserving map corresponding to a quantum physical evolution:

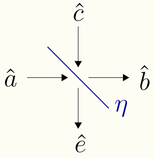
$$\rho_A \xrightarrow{\mathscr{N}} \rho_{BE}$$

Alice transmits a common message and a confidential message, m_0 and m_1, resp.
Bob — legitimate receiver of both m_0 and m_1
Eve — legitimate receiver of m_0, but also eavesdrops on m_1

Bosonic Model

For a single-mode bosonic broadcast channel, the channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the outputs are

$$\hat{b} = \sqrt{\eta}\,\hat{a} + \sqrt{1-\eta}\,\hat{c}$$
$$\hat{e} = \sqrt{1-\eta}\,\hat{a} - \sqrt{\eta}\,\hat{c}$$



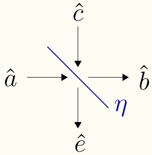
Bosonic Model

For a single-mode bosonic broadcast channel, the channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the outputs are

$$\hat{b} = \sqrt{\eta}\,\hat{a} + \sqrt{1-\eta}\,\hat{c}$$
$$\hat{e} = \sqrt{1-\eta}\,\hat{a} - \sqrt{\eta}\,\hat{c}$$

where

- the noise mode $\hat{c}$ is in a thermal Gaussian state (lossy) or vacuum state (pure-loss)



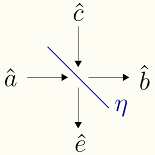
Bosonic Model

For a single-mode bosonic broadcast channel, the channel input is an electromagnetic field mode with annihilation operator $\hat{a}$, and the outputs are

$$\hat{b} = \sqrt{\eta}\,\hat{a} + \sqrt{1-\eta}\,\hat{c}$$
$$\hat{e} = \sqrt{1-\eta}\,\hat{a} - \sqrt{\eta}\,\hat{c}$$

where

- the noise mode $\hat{c}$ is in a thermal Gaussian state (lossy) or vacuum state (pure-loss)
- the transmissivity $\eta \in [0, 1]$ captures the absorption length of the optical fiber



Bosonic Model (Cont.)

- A coherent state $|\alpha\rangle$ corresponds to an oscillation of the electromagnetic field,

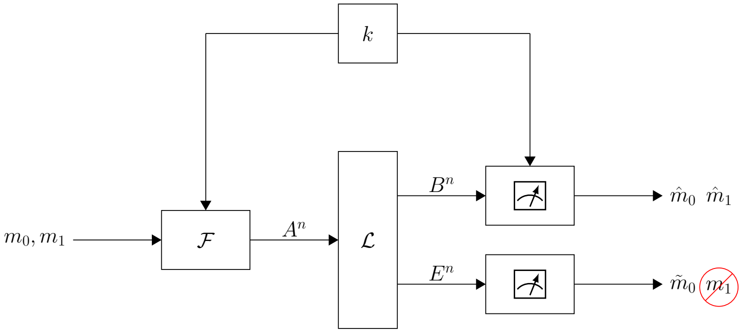
$$|\alpha\rangle = D(\alpha)|0\rangle$$
$$D(\alpha) \equiv \exp\left(\alpha \hat{a}^\dagger - \alpha^* \hat{a}\right)$$

- The transmitter employs a coherent state protocol.

Coding with Key Assistance

Communication Scheme (1)

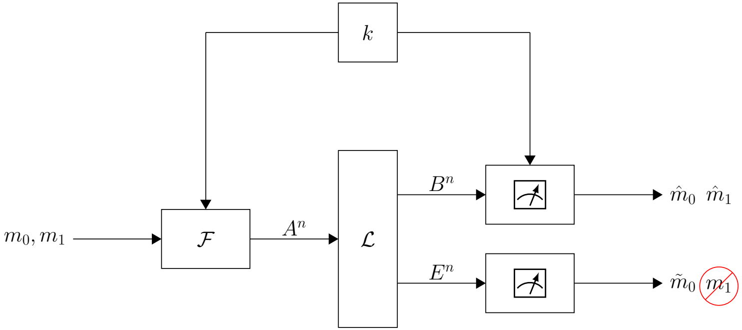
A key k is drawn from $[1:2^{nR_K}]$ uniformly at random, and then shared between Alice and Bob.



Coding with Key Assistance

Communication Scheme (2)

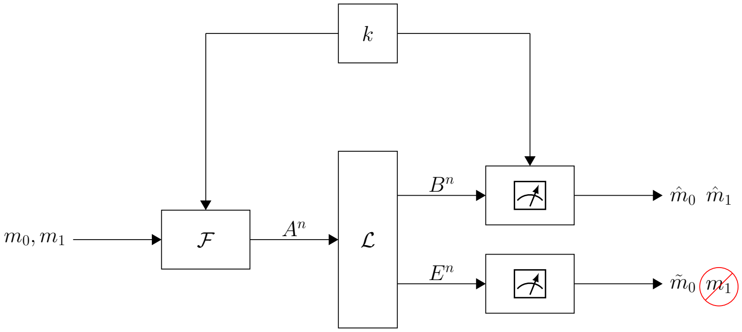
Alice chooses a common message m_0 for both Bob and Eve, and a confidential message m_1 for Bob.



Coding with Key Assistance

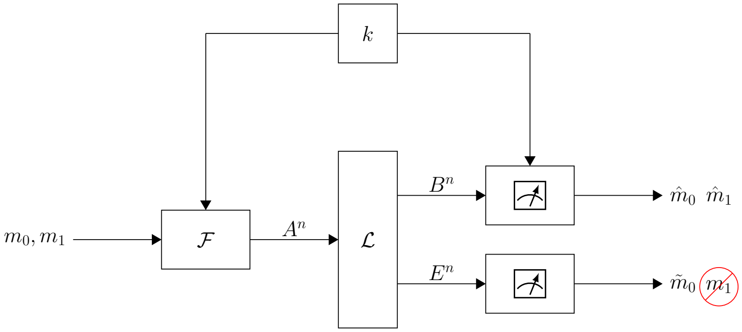
Communication Scheme (3)

Input: Alice prepares $\rho_{A^n}^{m_0,m_1,k} = \mathscr{F}(m_0, m_1, k)$, and transmits A^n.
Output: Bob and Eve receive B^n and E^n, resp.



Communication Scheme (4)

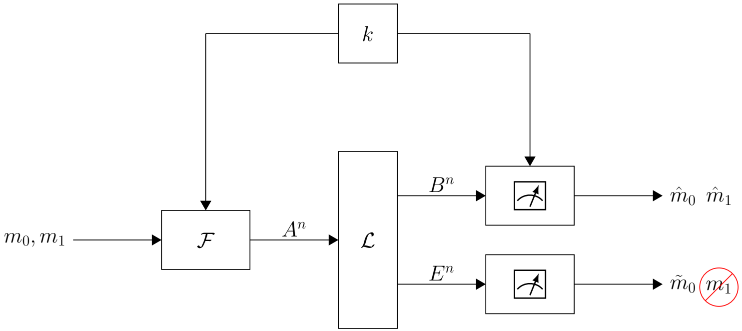
Eve performs a measurement Ξ_{E^n}, and obtains $\tilde{m}_0$.
Bob performs a measurement $\Gamma_{B^n|k}$, and obtains $\hat{m}_0, \hat{m}_1$.



Coding with Key Assistance

Security Requirement

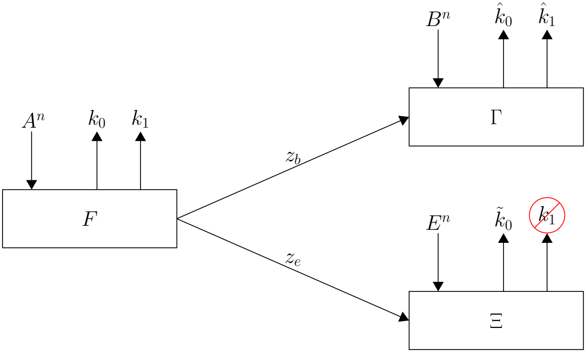
$$I(M_1; E^n | M_0)_\rho \to 0 \text{ as } n \to \infty$$



Conference Key Agreement

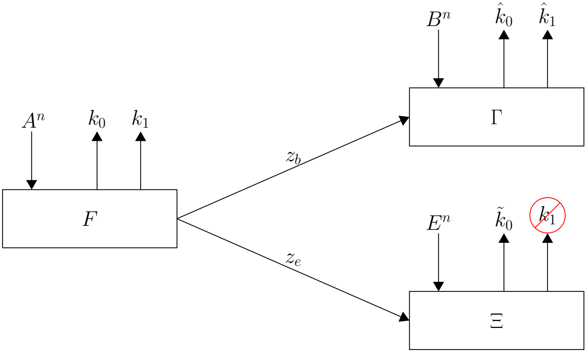
Key Agreement Protocol (1)

Alice, Bob, and Eve share a product state $\omega_{ABE}^{\otimes n}$.



Key Agreement Protocol (2)

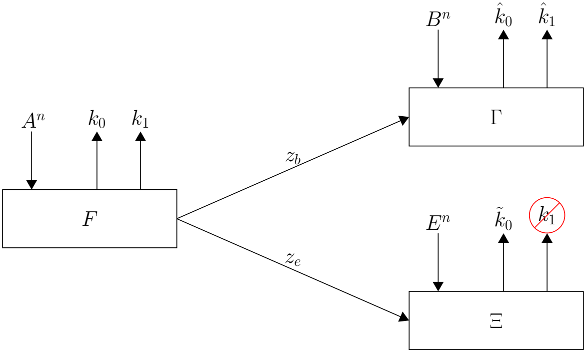
Alice performs a measurement F_{A^n}, producing k_0, k_1, z_b, z_e.



Conference Key Agreement

Key Agreement Protocol (3)

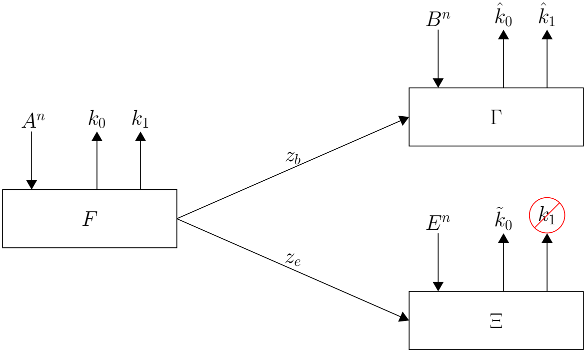
Alice sends z_b and z_e to Bob and Eve through a public channel.
Bob and Eve receive (B^n, z_b) and (E^n, z_e), resp.



Conference Key Agreement

Key Agreement Protocol (4)

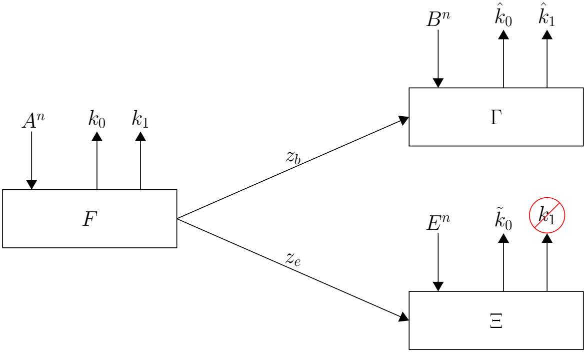
Eve performs a measurement $\Xi_{E^n|z_e}$, and obtains $\tilde{k}_0$.
Bob performs a measurement $\Gamma_{B^n|z_b}$, and obtains $\hat{k}_0, \hat{k}_1$.



Conference Key Agreement

Security Requirement

$$I(Z_b, Z_e; K_0)\,,\ I(Z_b, Z_e, E^n; K_1)_\rho \to 0 \text{ as } n \to \infty$$



Outline

- Key Assistance and Key Agreement
  - Definitions
  - Main Results
- Layered Secrecy
  - Channel Model
  - Main Results

Minimum Output Entropy Conjecture

Let $g(N)$ denote the entropy of a thermal state with mean photon number N, i.e.,

$$g(N) = \begin{cases} (N+1)\log(N+1) - N\log(N) & \text{if } N > 0 \\ 0 & \text{if } N = 0 \end{cases}$$

Minimum Output-Entropy Conjecture [Guha and Shapiro, 2007]

Given a pure-loss bosonic channel, if $H(A^n)_\rho = ng(N_A)$, then $H(B^n)_\rho \geq ng(\eta N_A)$.

Main Results: Key Assistance

Theorem (1)

Assume that the min output-entropy conjecture holds. Then, the capacity region of the pure-loss bosonic broadcast channel with confidential messages and key assistance is as follows. If $\eta \geq \frac{1}{2}$*, then*

$$\mathcal{C}(\mathscr{N}_{\textit{pure-loss}}) = \bigcup_{0\leq\beta\leq 1} \left\{ \begin{array}{rl} (R_0, R_1) \,:\, R_0 \leq & g((1-\eta)N_A) - g((1-\eta)\beta N_A) \\ R_1 \leq & g(\eta\beta N_A) - g((1-\eta)\beta N_A) + R_K \\ R_1 \leq & g(\eta\beta N_A) \end{array} \right\}.$$

Main Results: Key Assistance (Cont.)

Theorem (2)

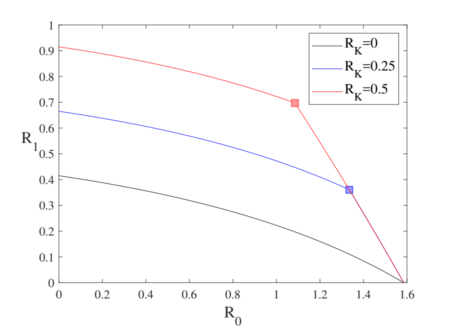
Otherwise, if $\eta < \frac{1}{2}$,

$$\mathcal{C}(\mathscr{N}_{\textit{pure-loss}}) = \bigcup_{0 \le \beta \le 1} \left\{ \begin{array}{rrl} (R_0, R_1) \; : & R_0 \le & g((1-\eta)N_A) - g((1-\eta)\beta N_A) \\ & R_1 \le & \min\left(g(\eta\beta N_A),\; R_K\right) \end{array} \right\}.$$

In this case, Bob has a noisier channel than Eve, and the confidential communication relies fully on the secret key (one-time pad).

Main Results: Key Assistance (Cont.)

Given the transmissivity $\eta = 0.6$ and input constraint $N_A = 5$:



For low common rates, the shared key is fully used to enhance the confidential communication. Whereas, for high rates, the key is only partially used.

The 'breaking point' corresponds to β_0 such that $g((1-\eta)\beta_0 N_A) = R_K$.

Main Results: Key Assistance (Cont.)

Proof outline

- Achievability is interpreted as a "superposition coding scheme", which consists of cloud centers $t^n(m_0)$ and satellites $x^n(m_0, m_1)$.
  - The cloud vector is chosen at random from a bin of size $2^{n[g((1-\eta)\beta N_A)+\delta]}$, to ensure that Eve can recover the cloud center, but not the satellite.
- The technical challenge is in the converse proof, which requires the min output-entropy conjecture. In the proof, it is applied to the degrading channel from Bob to Eve.

Main Results: Key Assistance (Cont.)

Remark

- The long-standing conjecture is known to hold in special cases, such as
  - $n = 1$ [De Palma, Trevisan, and Giovannetti, 2017]
  - $\rho_{A^n} = |\phi\rangle\langle\phi|$ [Giovannetti, Holevo, and García-Patrón, 2015]
- no longer needed for the single-user wiretap channel, i.e., for $R_0 = 0$ [Wilde and Qi, 2018]

Main Results: Key Agreement

Define the key-rate region,

$$\mathsf{K}(\omega_{ABE}) = \bigcup_{\Lambda_A,\, p_{T_0,T_1|X}} \left\{ \begin{array}{rl} (R_0, R_1) \,:\, R_0 \leq & \min\left(I(T_0;B)_\omega,\, I(T_0;E)_\omega\right) \\ R_1 \leq & [I(X;B|T_0,T_1)_\omega - I(X;E|T_0,T_1)_\omega]_+ \end{array} \right\}$$

where $[x]_+ = \max(x, 0)$, and the union is over the POVMs $\Lambda_A = \{\Lambda_A^x\}_{x\in\mathcal{X}}$ and distributions $p_{T_0,T_1|X}$, with

$$\omega_{BE}^{t_0,t_1,x} \equiv \mathrm{Tr}_A\left((\Lambda_A^x \otimes \mathbb{1} \otimes \mathbb{1})\omega_{ABE}\right).$$

Main Results: Key Agreement (Cont.)

Theorem

The key-agreement capacity region for the distillation of a public key and a secret key from ω_{ABE} in finite dimensions is given by

$$\mathcal{K}(\omega_{ABC}) = \bigcup_{n=1}^{\infty} \frac{1}{n} \mathsf{K}(\omega_{ABC}^{\otimes n}).$$

Main Results: Key Agreement (Cont.)

Theorem

The key-agreement capacity region for the distillation of a public key and a secret key from ω_{ABE} in finite dimensions is given by

$$\mathcal{K}(\omega_{ABC}) = \bigcup_{n=1}^{\infty} \frac{1}{n} \mathsf{K}(\omega_{ABC}^{\otimes n}).$$

Corollary

For a degraded broadcast channel,

$$\mathcal{C}_{\text{k-a}}(\mathcal{N}, 0) = \bigcup_{\omega_{ABE} \,:\, \omega_{BE} = \mathcal{N}_{A\to BE}(\omega_A)} \mathcal{K}(\omega_{ABC}).$$

Main Results: Key Agreement (Cont.)

Theorem

The key-agreement capacity region for the distillation of a public key and a secret key from ω_{ABE} in finite dimensions is given by

$$\mathcal{K}(\omega_{ABC}) = \bigcup_{n=1}^{\infty} \frac{1}{n} \mathsf{K}(\omega_{ABC}^{\otimes n}).$$

Corollary

For a degraded broadcast channel,

$$\mathcal{C}_{\text{k-a}}(\mathcal{N}, 0) = \bigcup_{\omega_{ABE} \,:\, \omega_{BE} = \mathcal{N}_{A \to BE}(\omega_A)} \mathcal{K}(\omega_{ABC}).$$

- In particular, for thermal states that are associated with a pure-loss bosonic channel, the key-agreement capacity region is a subset of the confidential capacity region with $R_K = 0$.

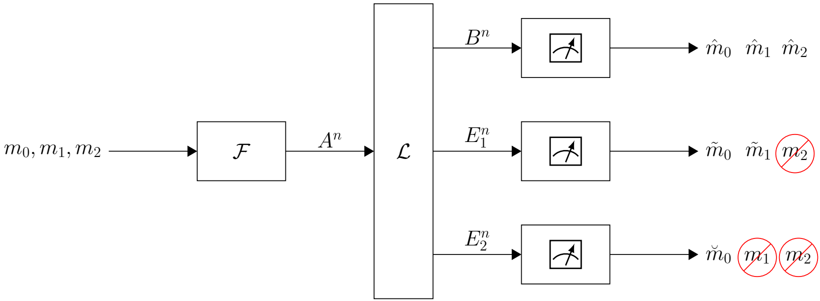
Outline

- Key Assistance and Key Agreement
  - Definitions
  - Main Results
- Layered Secrecy
  - Channel Model
  - Main Results

Coding with Layered Secrecy

Quantum Broadcast Channel with 3 Receivers

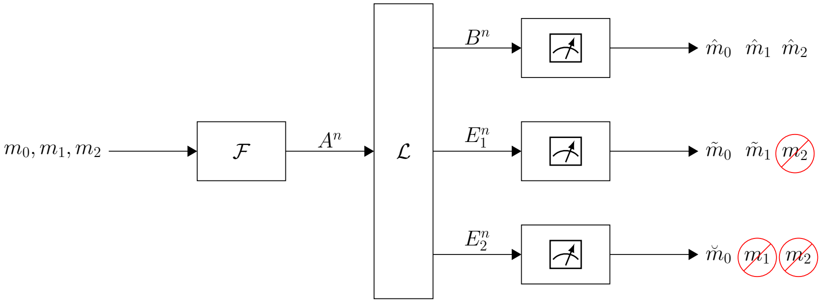
Consider a channel $\mathscr{N}_{A\to BE_1E_2}$ with three receivers, Bob, Eve 1, and Eve 2. Alice sends three messages.



Coding with Layered Secrecy

Layer-0

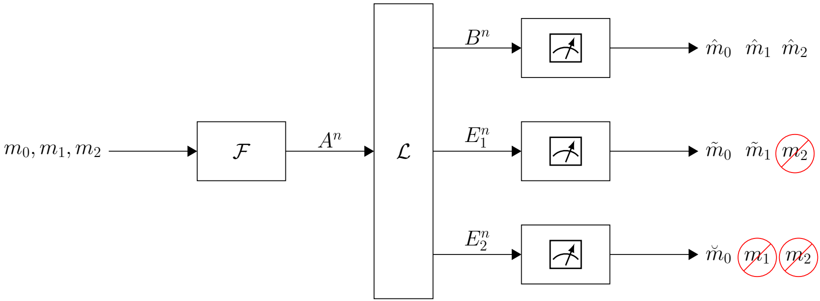
The common message m_0 is intended for all three receivers.



Coding with Layered Secrecy

Layer-1

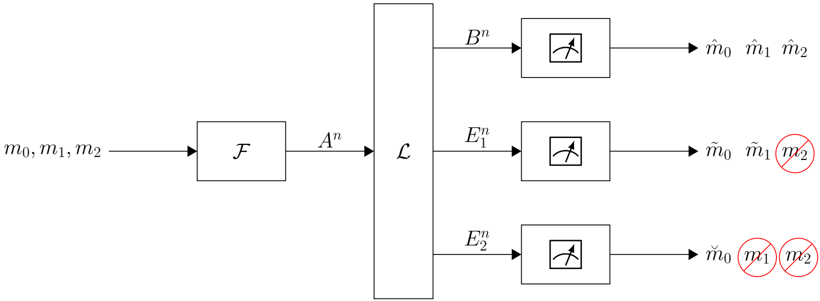
In the next layer, the confidential message m_1 is decoded by Bob and Eve 1, but should remain secret from Eve 2.



Coding with Layered Secrecy

Layer-2

The confidential message m_2 is decoded by Bob, but should remain secret from both Eve 1 and Eve 2.



Outline

Main Results: Layered Secrecy

Given a 3-receiver broadcast channel $\mathscr{N}_{A\to BE_1E_2}$, define the rate region,

$$\mathcal{R}_{\mathsf{LS}}(\mathscr{N}) = \bigcup_{p_{X_0,X_1,X_2}\,,\ \varphi_A^{x_0,x_1,x_2}} \left\{ \begin{array}{llll} (R_0,R_1,R_2): & R_0 \leq & I(X_0;E_2)_\rho \\ & R_1 \leq & [I(X_1;E_1|X_0)_\rho - I(X_1;E_2|X_0)_\rho]_+ \\ & R_2 \leq & [I(X_2;B|X_0,X_1)_\rho - I(X_2;E_1E_2|X_0,X_1)_\rho]_+ \end{array} \right\}$$

where the union is over the distribution p_{X_0,X_1,X_2}, and the state collections $\{\varphi_A^{x_0,x_1,x_2}\}$, with $\rho_{BE_1E_2}^{x_0x_1x_2} = \mathscr{N}_{A\to BE_1E_2}(\varphi_A^{x_0,x_1,x_2})$.

Main Results: Layered Secrecy (Cont.)

Theorem

The layered-secrecy capacity region of the quantum degraded broadcast channel $\mathscr{N}_{A\to BE_1E_2}$ in finite dimensions is given by

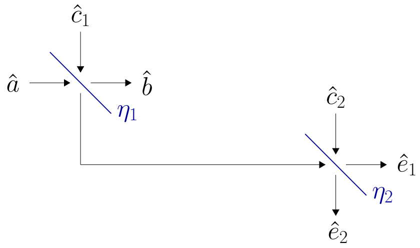
$$\mathcal{C}_{\mathsf{LS}}(\mathscr{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n} \mathcal{R}_{\mathsf{LS}}(\mathscr{N}^{\otimes n})$$

Main Results: Layered Secrecy (Cont.)

Theorem

A layered-secrecy rate tuple (R_0, R_1, R_2) is achievable over the pure-loss bosonic broadcast channel if

$$
\begin{aligned}
R_0 &\le g\big((1-\eta_1)(1-\eta_2)N_A\big) - g\big((\beta_1+\beta_2)(1-\eta_1)(1-\eta_2)N_A\big),\\
R_1 &\le g\big((\beta_1+\beta_2)\eta_2(1-\eta_1)N_A\big) - g\big(\beta_2\eta_2(1-\eta_1)N_A\big)\\
&\quad - \big[g\big((\beta_1+\beta_2)(1-\eta_2)(1-\eta_1)N_A\big) - g\big(\beta_2(1-\eta_2)(1-\eta_1)N_A\big)\big],\\
R_2 &\le g\big(\eta_1\beta_2 N_A\big) - g\big((1-\eta_1)\beta_2 N_A\big)\,, \text{ for some } \beta_1,\ \beta_2 \ge 0 \text{ s.t. } \beta_1+\beta_2 \le 1.
\end{aligned}
$$



Thank You!