Efficient Secret Key Distillation over Quantum Channels

arXiv: 1307.1136

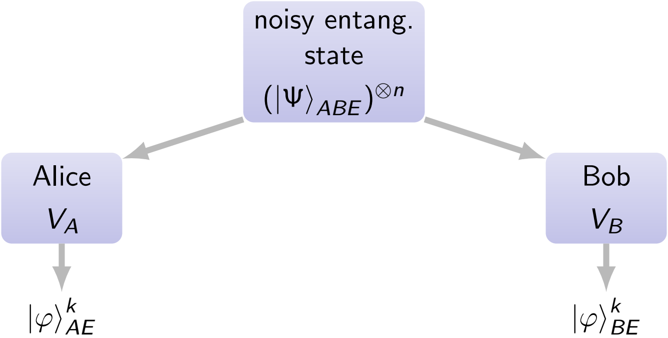
Joseph M. Renes*, David Sutter*, Frédéric Dupuis†, Renato Renner*

*Institute for Theoretical Physics, ETH Zurich
†Department of Computer Science, Aarhus University

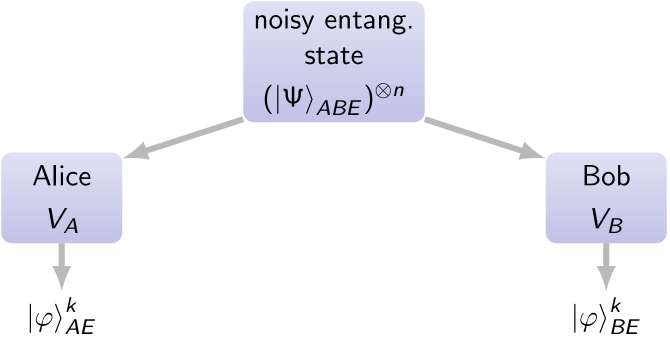
QCrypt 2014, Paris

ETH zürich

Secret-key distillation (SKD)

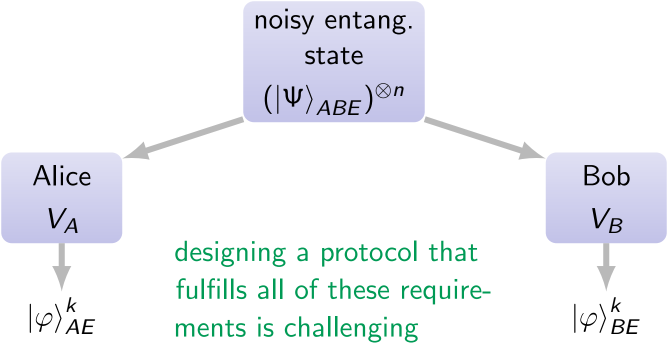


Secret-key distillation (SKD)



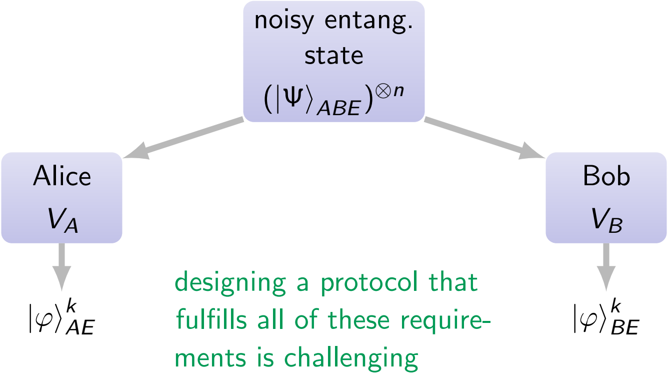
- **reliability:** $\varphi^k_A \approx \varphi^k_B$
- **secrecy:** no information about φ^k_A, φ^k_B leaks to environment
- **rate:** $\frac{k}{n}$ as high as possible
- **efficiency:** computationally cheap to run the protocol
- **additional ressources:** no preshared key required

Secret-key distillation (SKD)



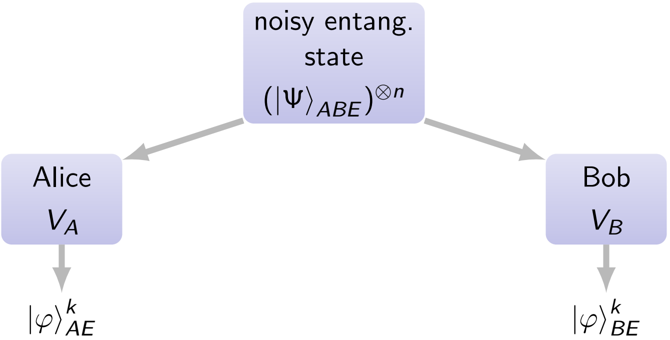
- **reliability:** $\varphi^k_A \approx \varphi^k_B$
- **secrecy:** no information about φ^k_A, φ^k_B leaks to environment
- **rate:** $\frac{k}{n}$ as high as possible
- **efficiency:** computationally cheap to run the protocol
- **additional ressources:** no preshared key required

Secret-key distillation (SKD)



- important primitive in quantum cryptography
- final step in most standard QKD protocols is a SKD task

Results: Overview



Explicit SKD protocol that

- is **reliable**
- is **secure**
- achieves the **private information**
- for Pauli or erasure noise has a complexity $\mathbf{O(n \log n)}$
- does **not need preshared key**

Outline

(classical) polar codes

- capacity achieving
- efficient encoding&decoding

↓

quantum polar codes

- CSS codes
- high rates & efficient

↓

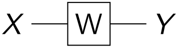
efficient entanglement distillation

↓

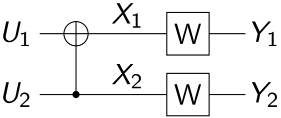
- shield system

efficient SKD

Polar codes — channel polarization [Arıkan'09]

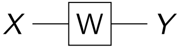


$I(\mathrm{W}) := I(X : Y)$

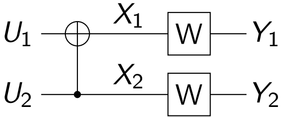


- for U_1, U_2 uniform $\underbrace{I(U_1 : Y_1 Y_2)}_{\leq I(\mathrm{W})} + \underbrace{I(U_2 : U_1 Y_1 Y_2)}_{\geq I(\mathrm{W})} = 2\, I(\mathrm{W})$

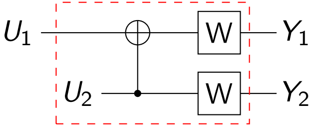
Polar codes — channel polarization [Arıkan'09]



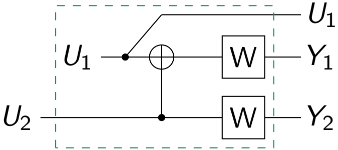
$I(\mathrm{W}) := I(X : Y)$



- for U_1, U_2 uniform $\underbrace{I(U_1 : Y_1 Y_2)}_{\leq I(\mathrm{W})} + \underbrace{I(U_2 : U_1 Y_1 Y_2)}_{\geq I(\mathrm{W})} = 2\, I(\mathrm{W})$
- define *logical* channels



worse channel W_-



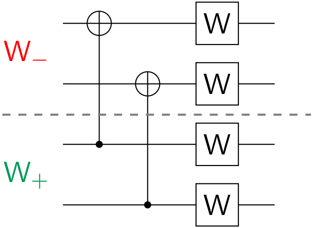
better channel W_+

- $I(\mathrm{W}_-) + I(\mathrm{W}_+) = 2I(\mathrm{W})$ with $I(\mathrm{W}_-) \leq I(\mathrm{W}) \leq I(\mathrm{W}_+)$

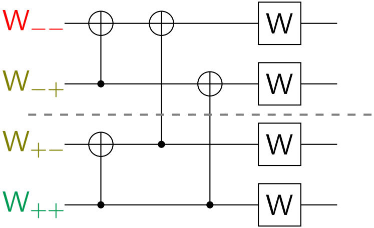
Polar codes — channel polarization [Arıkan'09] (con't)

- apply transformation recursively
- example $n = 4$

(i) divide channels in 2 groups & apply transf. in pairs

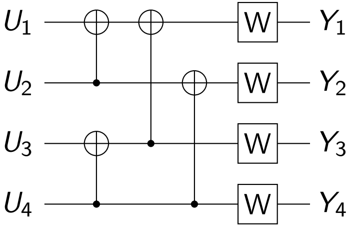


(ii) repeat for each type of channel



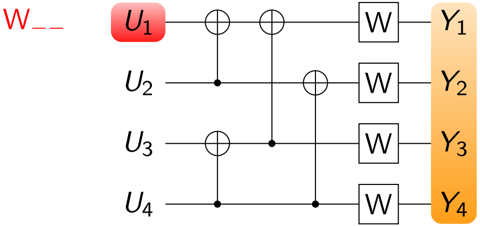
- inputs $\Leftrightarrow$ logical channels; e.g., U_3 is W_{+-}

Polar codes — channel polarization [Arıkan'09] (con't)



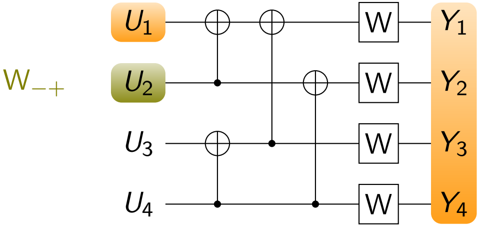
- logical outputs = all physical outputs & previous inputs

Polar codes — channel polarization [Arıkan'09] (con't)



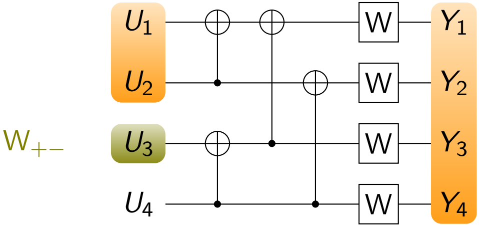
- logical outputs = all physical outputs & previous inputs

Polar codes — channel polarization [Arıkan'09] (con't)



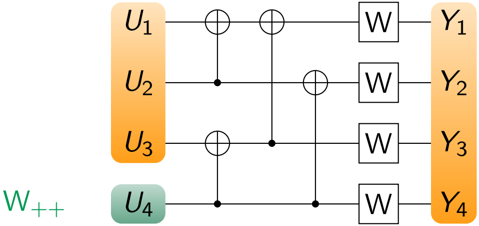
- logical outputs = all physical outputs & previous inputs

Polar codes — channel polarization [Arıkan'09] (con't)



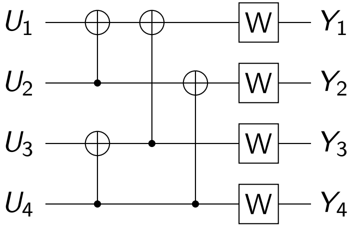
- logical outputs = all physical outputs & previous inputs

Polar codes — channel polarization [Arıkan'09] (con't)



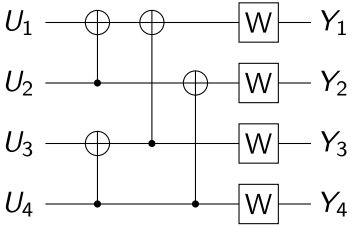
- logical outputs = all physical outputs & previous inputs

Polar codes — channel polarization [Arıkan'09] (con't)



- logical outputs = all physical outputs & previous inputs
- **Polarization Phenomenon (informal)**: As $n \to \infty$ essentially all logical channels are either almost perfect or almost pure noise.

Polar codes — channel polarization [Arıkan'09] (con't)

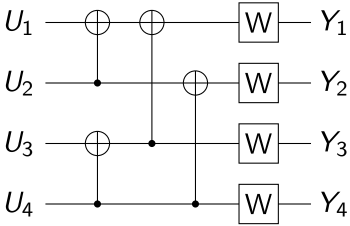


- logical outputs = all physical outputs & previous inputs
- **Polarization Phenomenon (informal)**: As $n \to \infty$ essentially all logical channels are either almost perfect or almost pure noise.
- **Polarization Phenomenon (formal)**: For every $\varepsilon \in (0,1)$

$$\lim_{n\to\infty} \frac{1}{n} \left| \left\{ i \in [n] : I\left(U_i : Y^n U^{i-1}\right) \in (\varepsilon, 1-\varepsilon) \right\} \right| = 0$$

- fraction of good channels is $= I(\mathrm{W})$ (= capacity of W)

Polar codes — channel polarization [Arıkan'09] (con't)



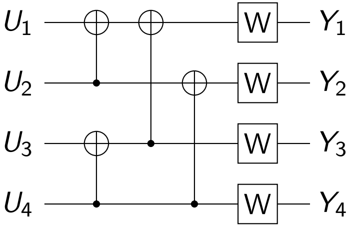
- send messages over good channels
- freeze inputs to bad channels to 0
- $O(n \log n)$ CNOTs
  - logical outputs = all physical outputs & previous inputs
  - **Polarization Phenomenon (informal)**: As $n \to \infty$ essentially all logical channels are either almost perfect or almost pure noise.
  - **Polarization Phenomenon (formal)**: For every $\varepsilon \in (0,1)$

$$\lim_{n\to\infty} \frac{1}{n} \left| \left\{ i \in [n] : I\left(U_i : Y^n U^{i-1}\right) \in (\varepsilon, 1-\varepsilon) \right\} \right| = 0$$

  - fraction of good channels is $= I(\mathrm{W})$ ($=$ capacity of W)

Polar codes — channel polarization [Arıkan'09] (con't)

- send messages over good channels
- freeze inputs to bad channels to 0
- $O(n \log n)$ CNOTs



- decode sequentially using max. likelihood
- recursive structure makes ML efficient
- $O(n \log n)$
- $p_{\mathrm{err}} = O(2^{-\sqrt{n}})$

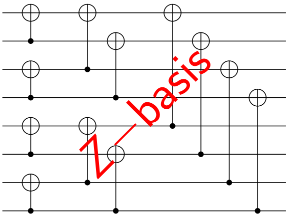
- logical outputs = all physical outputs & previous inputs
- **Polarization Phenomenon (informal)**: As $n \to \infty$ essentially all logical channels are either almost perfect or almost pure noise.
- **Polarization Phenomenon (formal)**: For every $\varepsilon \in (0, 1)$

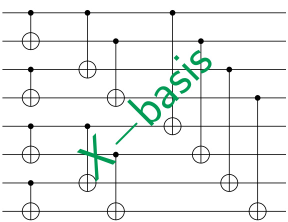
$$\lim_{n \to \infty} \frac{1}{n} \left| \left\{ i \in [n] : I\left(U_i : Y^n U^{i-1}\right) \in (\varepsilon, 1 - \varepsilon) \right\} \right| = 0$$

- fraction of good channels is $= I(\mathrm{W})$ ($=$ capacity of W)

Quantum polar codes

- Polarization occurs in Z (amplitude) and X (phase) basis





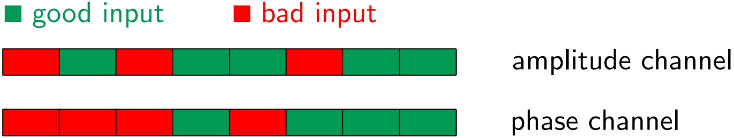
- Z and X bases $\rightarrow$ send entanglement [Christandl&Winter'05]
- Shown to be applicable for several different information processing tasks [Dupuis-Guha-Renes-Renner-Wilde-...]

Quantum polar codes (con't)

- Determine induced amplitude and phase channel
  - $\mathcal{Q}$:= indices good for amplitude & good for phase
  - $\mathcal{A}$:= indices good for amplitude & bad for phase
  - $\mathcal{P}$:= indices bad for amplitude & good for phase
  - $\mathcal{E}$:= indices bad for amplitude & bad for phase

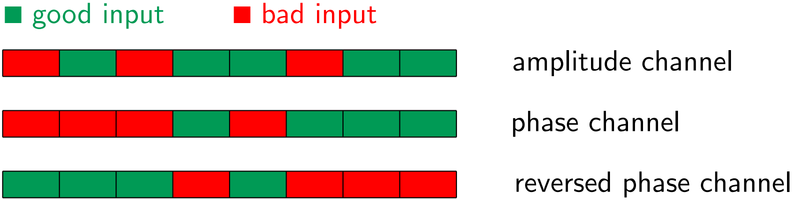
Quantum polar codes (con't)

- Determine induced amplitude and phase channel
  - $\mathcal{Q}$:= indices good for amplitude & good for phase
  - $\mathcal{A}$:= indices good for amplitude & bad for phase
  - $\mathcal{P}$:= indices bad for amplitude & good for phase
  - $\mathcal{E}$:= indices bad for amplitude & bad for phase



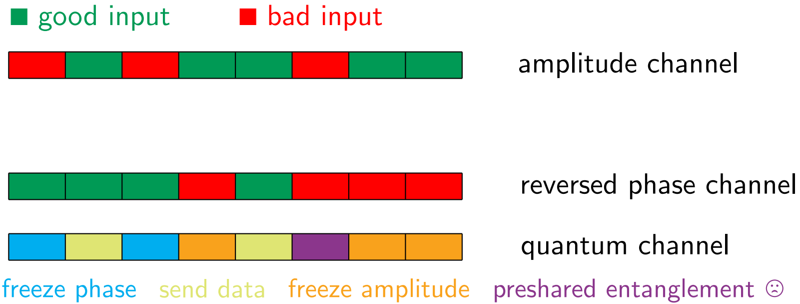
Quantum polar codes (con't)

- Determine induced amplitude and phase channel
  - $\mathcal{Q}$:= indices good for amplitude & good for phase
  - $\mathcal{A}$:= indices good for amplitude & bad for phase
  - $\mathcal{P}$:= indices bad for amplitude & good for phase
  - $\mathcal{E}$:= indices bad for amplitude & bad for phase



Quantum polar codes (con't)

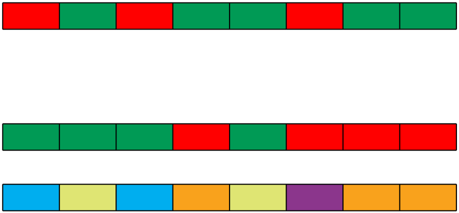
- Determine induced amplitude and phase channel
  - $\mathcal{Q}$:= indices good for amplitude & good for phase
  - $\mathcal{A}$:= indices good for amplitude & bad for phase
  - $\mathcal{P}$:= indices bad for amplitude & good for phase
  - $\mathcal{E}$:= indices bad for amplitude & bad for phase



Quantum polar codes (con't)

- Determine induced amplitude and phase channel
  - $\mathcal{Q}$:= indices good for amplitude & good for phase
  - $\mathcal{A}$:= indices good for amplitude & bad for phase
  - $\mathcal{P}$:= indices bad for amplitude & good for phase
  - $\mathcal{E}$:= indices bad for amplitude & bad for phase

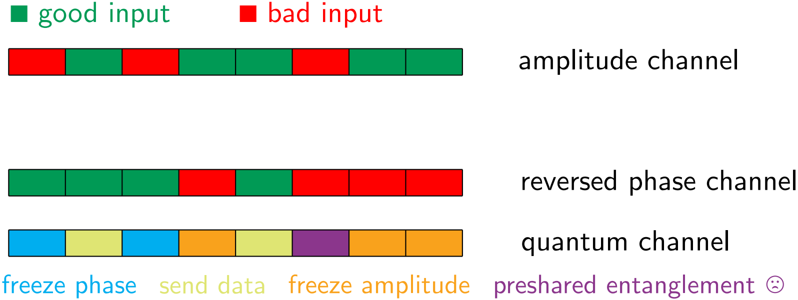
■ good input ■ bad input



- $\exists$ channels with [Hassani-Renes-DS'14]
  - $|\mathcal{E}| = o(n)$ (e.g., degradable channels)
  - $|\mathcal{E}| = O(n)$ (e.g., depolarizing channel)

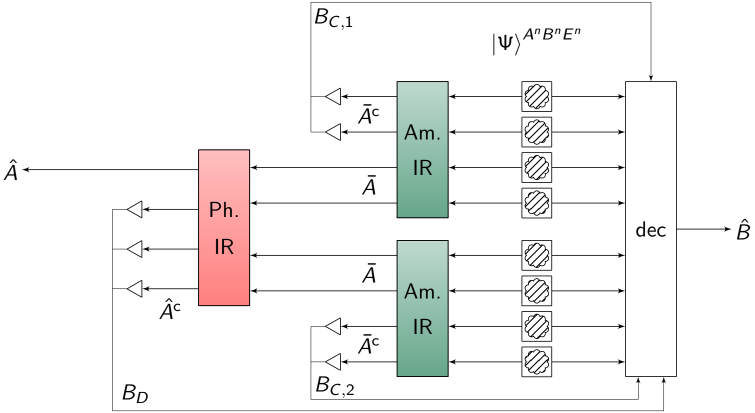
Quantum polar codes (con't)

- Determine induced amplitude and phase channel
  - $\mathcal{Q}$:= indices good for amplitude & good for phase
  - $\mathcal{A}$:= indices good for amplitude & bad for phase
  - $\mathcal{P}$:= indices bad for amplitude & good for phase
  - $\mathcal{E}$:= indices bad for amplitude & bad for phase



- $\exists$ channels with [Hassani-Renes-DS'14]
  - $|\mathcal{E}| = o(n)$ (e.g., degradable channels)
  - $|\mathcal{E}| = O(n)$ (e.g., depolarizing channel)
- **Solution:** concatenated protocol with two polarization steps

Entanglement Distillation ($\ell = 4$, m = 2)



- Amplitude IR: $p_{\mathrm{err}}\left(Z^{A^n}|B^n B_C^m\right) \leq m\epsilon_1$
- Phase IR: $p_{\mathrm{err}}\left(X^{\bar{A}^m}|B^n C^n B_D\right) \leq \epsilon_2$

Entanglement Distillation: Characteristics

- Rate: $R := \frac{\#\text{ qubits at output}}{n} \geq I(A\rangle B)_\psi$
- Reliability: $\delta\left(|\phi\rangle_d^{\hat{A}\hat{B}}, \mathcal{F}\left(\Psi^{A^nB^nE^n}\right)\right) \leq \sqrt{2\epsilon_2} + \sqrt{2m\epsilon_1}$

$m = \#$ inner blocks

$\ell = \#$ inputs per inner block

$n = m\ell$ blocklength

Entanglement Distillation: Characteristics

- Rate: $R := \frac{\#\text{ qubits at output}}{n} \geq I(A\rangle B)_\psi$
- Reliability: $\delta\left(|\phi\rangle_d^{\hat{A}\hat{B}}, \mathcal{F}\left(\Psi^{A^n B^n E^n}\right)\right) \leq \sqrt{2\epsilon_2} + \sqrt{2m\epsilon_1}$

max. entang-
led state

output state
from protocol

$m = \#$ inner blocks

$\ell = \#$ inputs per inner block

$n = m\ell$ blocklength

Entanglement Distillation: Characteristics

- Rate: $R := \frac{\#\text{ qubits at output}}{n} \geq I(A\rangle B)_\psi$
- Reliability: $\delta\left(|\phi\rangle_d^{\hat{A}\hat{B}}, \mathcal{F}\left(\Psi^{A^n B^n E^n}\right)\right) \leq \sqrt{2\epsilon_2} + \sqrt{2m\epsilon_1}$

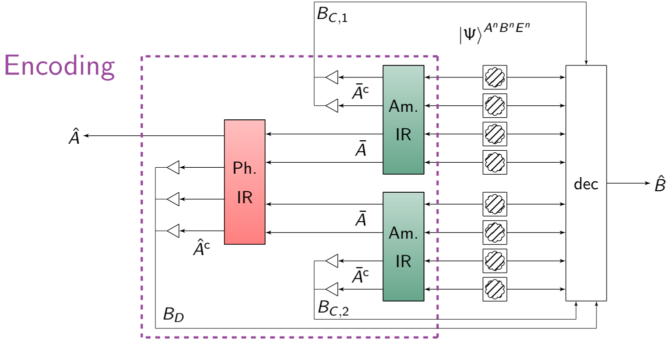
  $\uparrow$ max. entangled state

  $\uparrow$ output state from protocol

  $m = \#$ inner blocks
  $\ell = \#$ inputs per inner block
  $n = m\ell$ blocklength

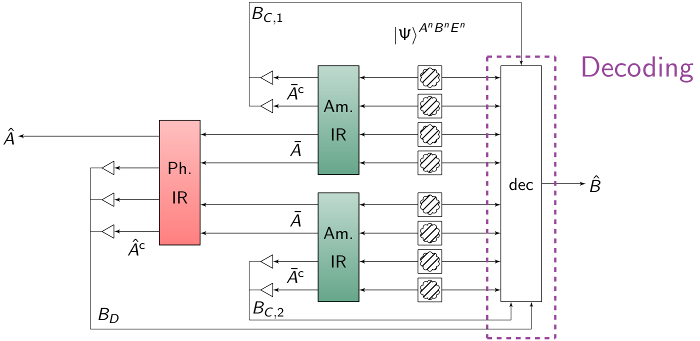
- Using Quantum Polar Codes:
  - $\epsilon_1 = O\left(2^{-\sqrt{\ell}}\right)$ and $\epsilon_2 = O\left(\ell\, 2^{-\sqrt{m}}\right)$
  - For Pauli and erasure noise the complexity of the scheme is $O(n \log n)$.

Efficient Encoding and Decoding using Polar Codes

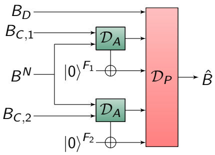


- Inner layer: standard polar encoder
- Outer layer: multilevel polarization encoder

Efficient Encoding and Decoding using Polar Codes



$\mathcal{D}_A$: Use the standard polar decoder [Arıkan'09]



$\mathcal{D}_P$: Use the decoder for a classical concatenated polar coding scheme [DS-Renes-Dupuis-Renner'12]

Efficient secret-key distillation

- If Alice and Bob share a *shield* system S
- Entanglement distillation $\rightarrow$ secret-key distillation
- Secrecy ensured via uncertainty principle
- Rate $R \geq H\big(Z^A|E\big) - H\big(Z^A|B\big)$
- Computationally efficient for Pauli and erasure noise using polar codes $O(n \log n)$
- No preshared secret key is needed

Efficient secret-key distillation

Any system not held by Eve that however cannot be used for amplitude IR by Alice and Bob

- If Alice and Bob share a *shield* system S
- Entanglement distillation $\rightarrow$ secret-key distillation
- Secrecy ensured via uncertainty principle
- Rate $R \geq H(Z^A|E) - H(Z^A|B)$
- Computationally efficient for Pauli and erasure noise using polar codes $O(n \log n)$
- No preshared secret key is needed

Summary & Outlook

arXiv:1307.1136

- Efficient protocol for entanglement distillation at (almost) optimal rate
- Useful for efficient SKD at private information
- Quantum communication at coherent information
  - efficient for Pauli and erasure channels
  - no entanglement assistance needed
- Can it be efficient for arbitrary noise?