

Efficient Secret Key Distillation over Quantum Channels

arXiv: 1307.1136

Joseph M. Renes^{*}, David Sutter^{*}, Frédéric Dupuis[†], Renato Renner^{*}

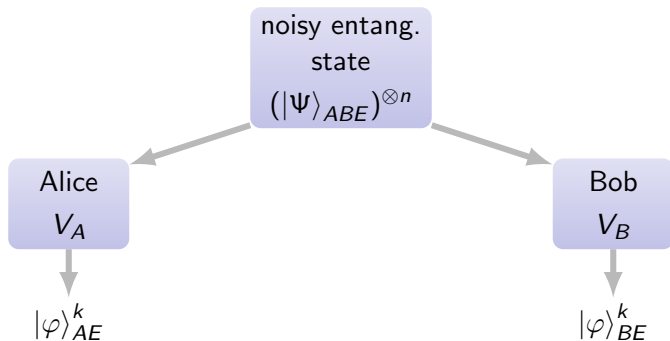
^{*}Institute for Theoretical Physics, ETH Zurich

[†]Department of Computer Science, Aarhus University

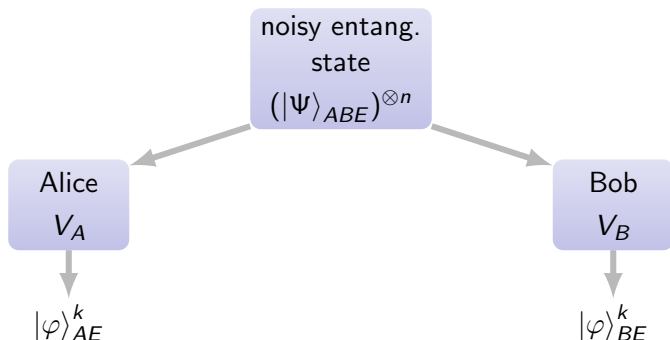
QCrypt 2014, Paris

ETH zürich

Secret-key distillation (SKD)

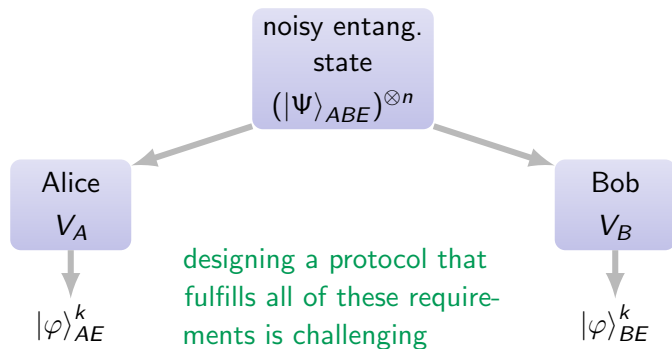


Secret-key distillation (SKD)



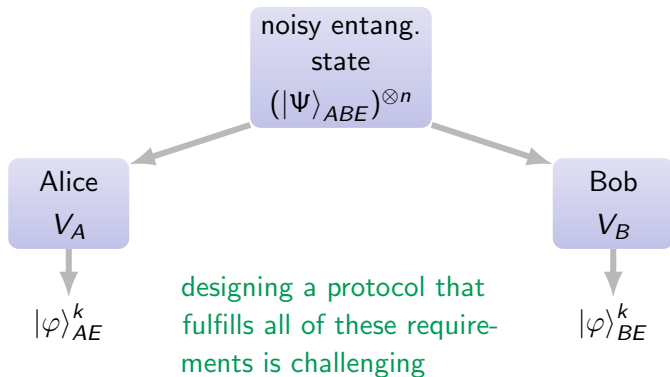
- ▶ **reliability:** $\varphi_A^k \approx \varphi_B^k$
- ▶ **secrecy:** no information about φ_A^k, φ_B^k leaks to environment
- ▶ **rate:** $\frac{k}{n}$ as high as possible
- ▶ **efficiency:** computationally cheap to run the protocol
- ▶ **additional resources:** no preshared key required

Secret-key distillation (SKD)



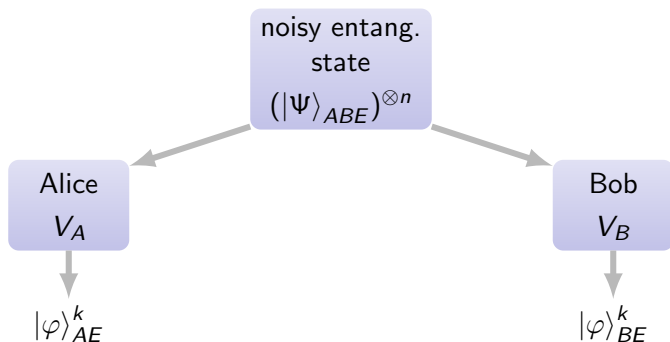
- ▶ **reliability:** $\varphi_A^k \approx \varphi_B^k$
- ▶ **secrecy:** no information about φ_A^k, φ_B^k leaks to environment
- ▶ **rate:** $\frac{k}{n}$ as high as possible
- ▶ **efficiency:** computationally cheap to run the protocol
- ▶ **additional resources:** no preshared key required

Secret-key distillation (SKD)



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

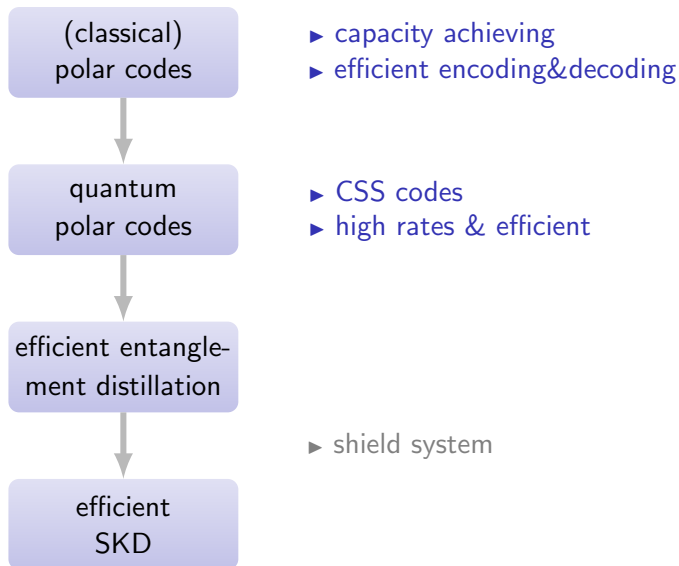
Results: Overview



Explicit SKD protocol that

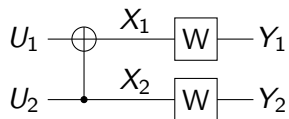
- ▶ is **reliable**
- ▶ is **secure**
- ▶ achieves the **private information**
- ▶ for Pauli or erasure noise has a complexity **$O(n \log n)$**
- ▶ does **not need preshared key**

Outline



Polar codes — channel polarization [Arıkan'09]

$$X \text{ --- } \boxed{W} \text{ --- } Y$$
$$I(W) := I(X : Y)$$

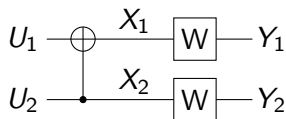


- for U_1, U_2 uniform $\underbrace{I(U_1 : Y_1 Y_2)}_{\leq I(W)} + \underbrace{I(U_2 : U_1 Y_1 Y_2)}_{\geq I(W)} = 2 I(W)$

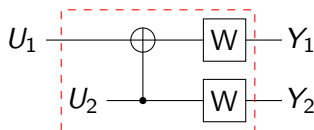
Polar codes — channel polarization [Arıkan'09]

$$X \text{ --- } \boxed{W} \text{ --- } Y$$

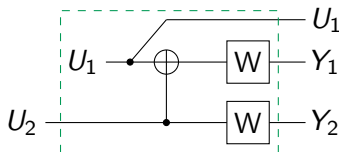
$$I(W) := I(X : Y)$$



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



worse channel W_-



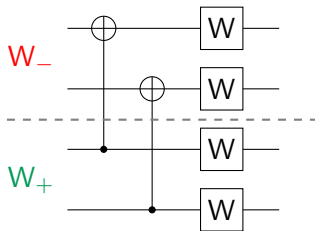
better channel W_+

- ▶ $I(W_-) + I(W_+) = 2I(W)$ with $I(W_-) \leq I(W) \leq I(W_+)$

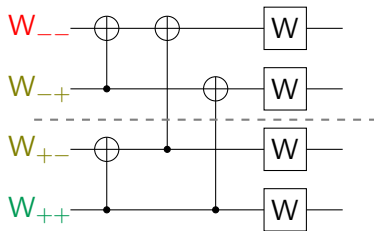
Polar codes — channel polarization [Arıkan'09] (con't)

- ▶ apply transformation recursively
- ▶ example $n = 4$

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

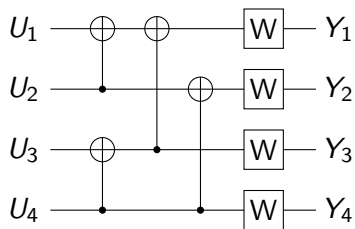


(ii) repeat for each type
of channel



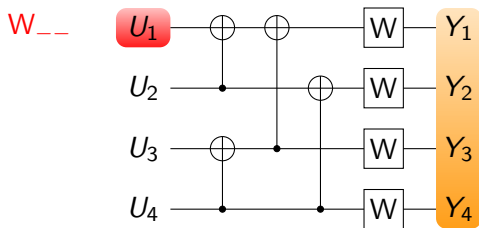
- ▶ inputs \Leftrightarrow logical channels; e.g., U_3 is W_{+-}

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



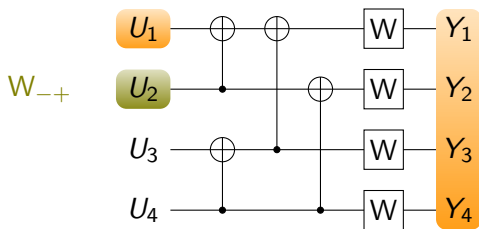
- ▶ **logical outputs** = all physical outputs & previous inputs

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



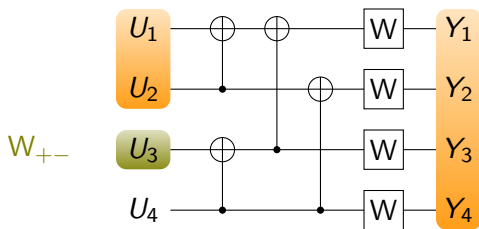
- ▶ **logical outputs** = all physical outputs & previous inputs

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



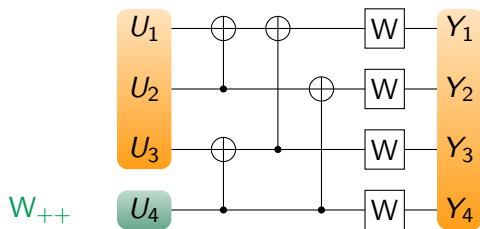
- ▶ **logical outputs** = all physical outputs & previous inputs

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



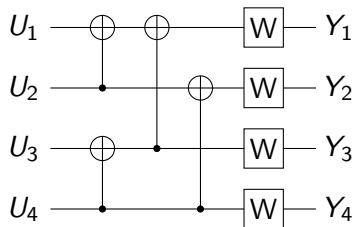
- ▶ **logical outputs** = all physical outputs & previous inputs

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



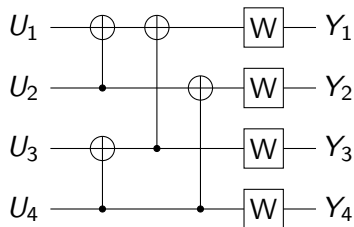
- ▶ **logical outputs** = all physical outputs & previous inputs

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



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

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

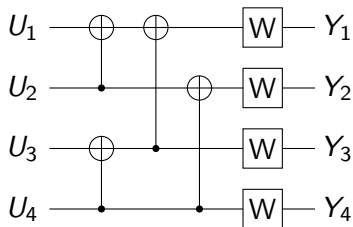
- ▶ fraction of good channels is = $I(W)$ (= capacity of W)

Polar codes — channel polarization [Arikan'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 $n \rightarrow \infty$ essentially all logical channels are either **almost perfect** or **almost pure noise**.

► **Polarization Phenomenon (formal)**: For every $\varepsilon \in (0, 1)$

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

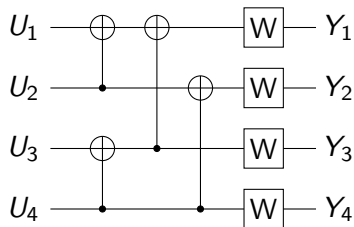
► fraction of good channels is $= I(W)$ (= capacity of W)

Polar codes — channel polarization [Arikan'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

► $O(n \log n)$

► $p_{\text{err}} = O(2^{-\sqrt{n}})$

► **logical outputs** = all physical outputs & previous inputs

► **Polarization Phenomenon (informal)**: As $n \rightarrow \infty$ essentially all logical channels are either **almost perfect** or **almost pure noise**.

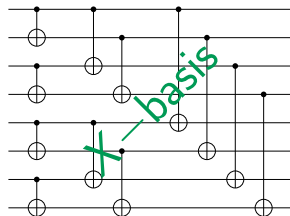
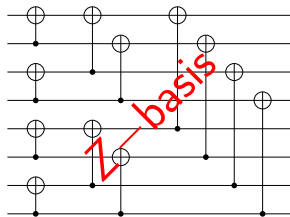
► **Polarization Phenomenon (formal)**: For every $\varepsilon \in (0, 1)$

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

► fraction of good channels is $= I(W)$ (= 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

■ good input ■ bad input



amplitude channel



phase 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

■ good input ■ bad input



amplitude channel



phase channel



reversed phase 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

■ good input ■ bad input



amplitude channel



reversed phase channel



quantum channel

freeze phase send data freeze amplitude preshared entanglement ☹

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



amplitude channel



reversed phase channel



quantum channel

freeze phase send data freeze amplitude preshared entanglement ☹

- ▶ \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

■ good input ■ bad input



amplitude channel



reversed phase channel

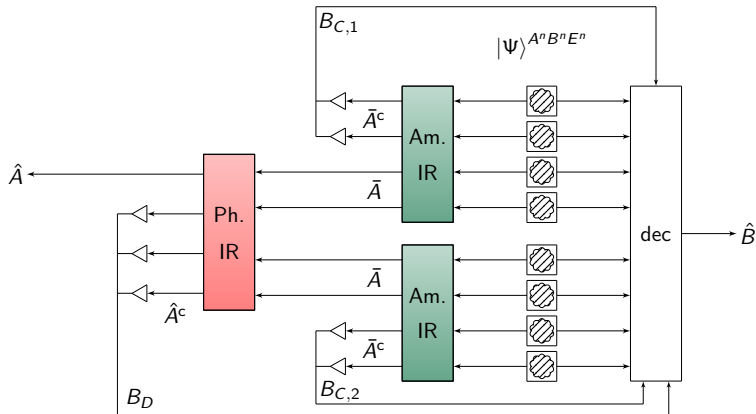


quantum channel

freeze phase send data freeze amplitude preshared entanglement ☹

- ▶ \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:** $p_{\text{err}}(Z^{A^n} | B^n B_C^m) \leq m\epsilon_1$

► **Phase IR:** $p_{\text{err}}(X^{\bar{A}^m} | B^n C^n B_D) \leq \epsilon_2$

Entanglement Distillation: Characteristics

► Rate: $R := \frac{\# \text{ qubits at output}}{n} \geq I(A)B)_\psi$

► Reliability: $\delta \left(|\phi\rangle_d^{\hat{A}\hat{B}}, \mathcal{F}(\Psi^{A^n B^n E^n}) \right) \leq \sqrt{2\epsilon_2} + \sqrt{2m\epsilon_1}$

$m = \#$ 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: $\delta \left(\underbrace{|\phi\rangle_d^{\hat{A}\hat{B}}}_{\text{max. entangled state}}, \underbrace{\mathcal{F}(\Psi^{A^n B^n E^n})}_{\text{output state from protocol}} \right) \leq \sqrt{2\epsilon_2} + \sqrt{2m\epsilon_1}$

max. entangled state

output state from protocol

$m = \#$ inner blocks

$\ell = \#$ inputs per inner block

$n = m\ell$ blocklength

Entanglement Distillation: Characteristics

▶ Rate: $R := \frac{\# \text{ qubits at output}}{n} \geq I(A)B)_\psi$

▶ Reliability: $\delta \left(\left| \phi \right\rangle_d^{\hat{A}\hat{B}}, \mathcal{F} \left(\Psi^{A^n B^n E^n} \right) \right) \leq \sqrt{2\epsilon_2} + \sqrt{2m\epsilon_1}$

max. entang-
led state

output state
from protocol

$m = \#$ inner blocks

$\ell = \#$ inputs per inner block

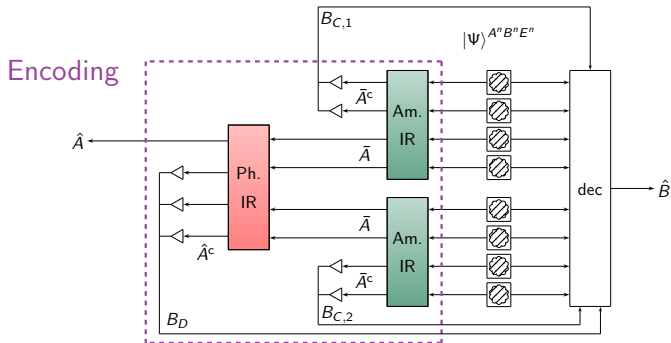
$n = m\ell$ blocklength

▶ Using Quantum Polar Codes:

▶ $\epsilon_1 = O\left(2^{-\sqrt{\ell}}\right)$ and $\epsilon_2 = O\left(\ell 2^{-\sqrt{m}}\right)$

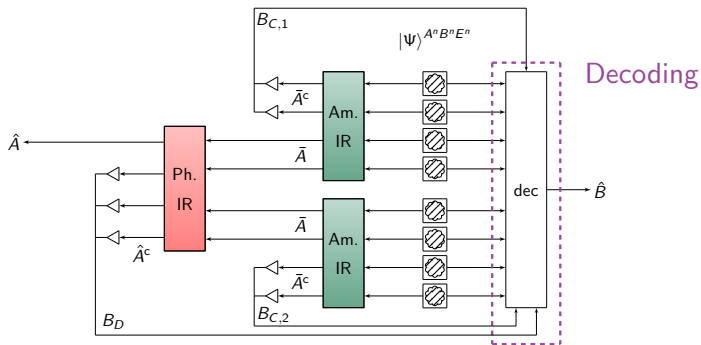
▶ For Pauli and erasure noise the complexity of the scheme is $O(n \log n)$.

Efficient Encoding and Decoding using Polar Codes

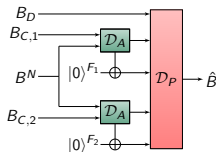


- ▶ Inner layer: standard polar encoder
- ▶ Outer layer: multilevel polarization encoder

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 $R \geq H(Z^A|E) - H(Z^A|B)$
- ▶ Computationally efficient for Pauli and erasure noise using polar codes $O(n \log n)$
- ▶ No preshared secret key is needed

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?