Entanglement

Rafał Demkowicz-Dobrzański

Nicolaus Copernicus University, Toruń, Poland

Aditi Sen (De), Ujjwal Sen, Maciej Lewnestein

ICFO-Institut de Ciencies Fotoniques, Barcelona, Spain

Entanglement enhances security in secret sharing
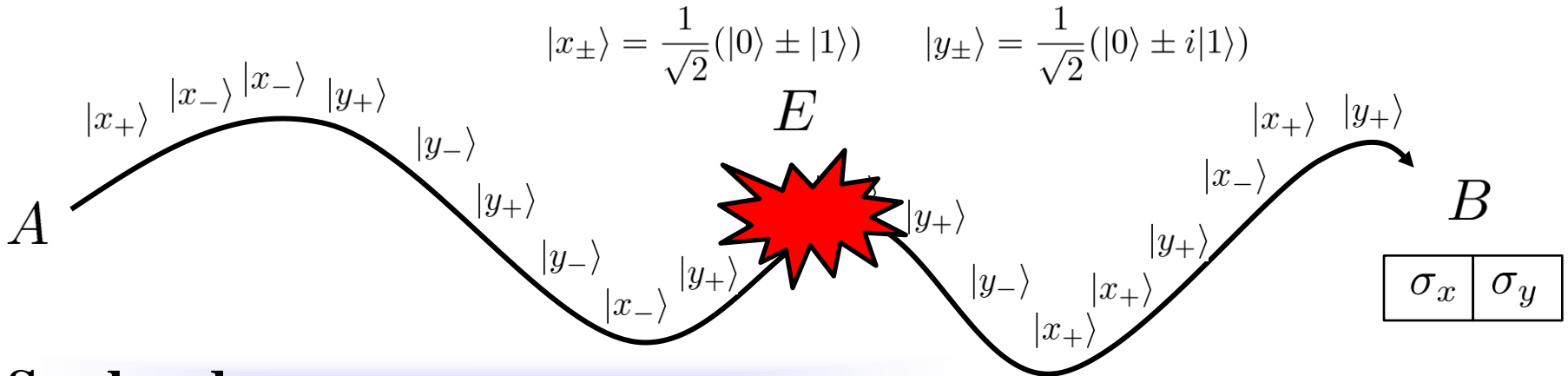
Rafał Demkowicz-Dobrzański

Nicolaus Copernicus University, Toruń, Poland

Aditi Sen (De), Ujjwal Sen, Maciej Lewnestein

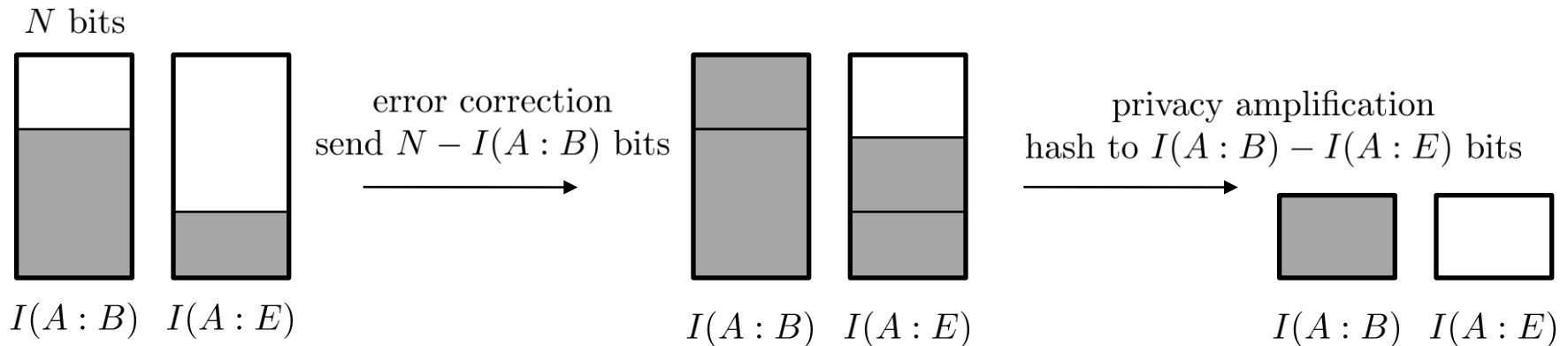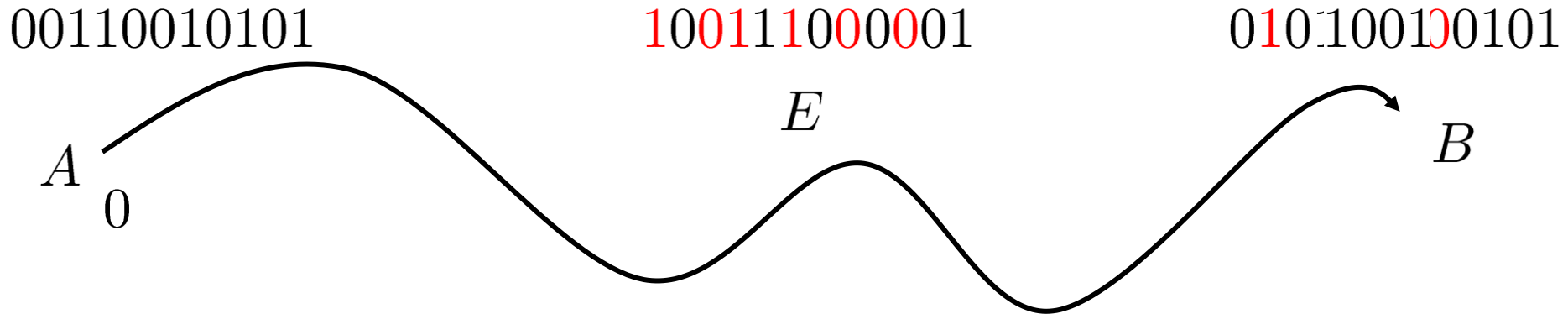*ICFO-Institut de Ciencies Fotoniques, Barcelona, Spain*

BB84 QKD

$$|x_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \qquad |y_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$$

Send and measure

A key	0	0			1			0		0
A	x_+	y_+	y_+	y_-	x_-	x_-	x_+	y_+	y_+	x_+
B	σ_x	σ_y	σ_x	σ_x	σ_x	σ_y	σ_y	σ_y	σ_x	σ_x
compatible?	✓	✓			✓			✓		✓
B key	0	1			1			1		0

Remove bits obtained in incompatible basis

Reveal part of bits to estimate QBER

If low enough, perform error-correction + privacy amplification

Error correction + privacy amplification

00110010101   10011100001   01010010101

A

E

B

0

N bits

error correction
send $N - I(A:B)$ bits

$I(A:B)$ $I(A:E)$

$I(A:B)$ $I(A:E)$

privacy amplification
hash to $I(A:B) - I(A:E)$ bits

$I(A:B)$ $I(A:E)$

N noisy unsecure bits   ->   I(A:B)-I(A:E) error free secure bits

Key generation rate in QKD
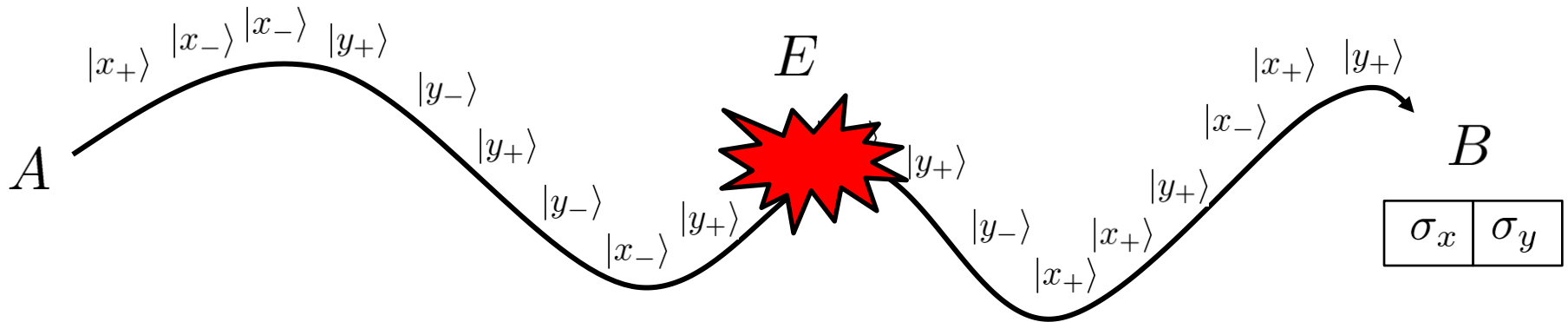
Assuming individual attacks, one-way error correction, privacy amplification, the key rate is bounded (Csiszar-Koerner):

$$K \leq \max[I(A:B) - I(A:E), I(A:B) - I(B:E)])$$

QBER threshold for BB84:

$$I(A:B) = I(A:E) = I(B:E)$$

$$QBER = \frac{1 - 1/\sqrt{2}}{2} \approx 14.6\%$$

Is entanglement useful in QKD

• Entanglement based QKD protocols (e.g. Ekert) yield the same QBER thresholds as the corresponding prepare and measure protocols (e.g. BB84)

• Entanglement proves useful only when considering device independent secure QKD

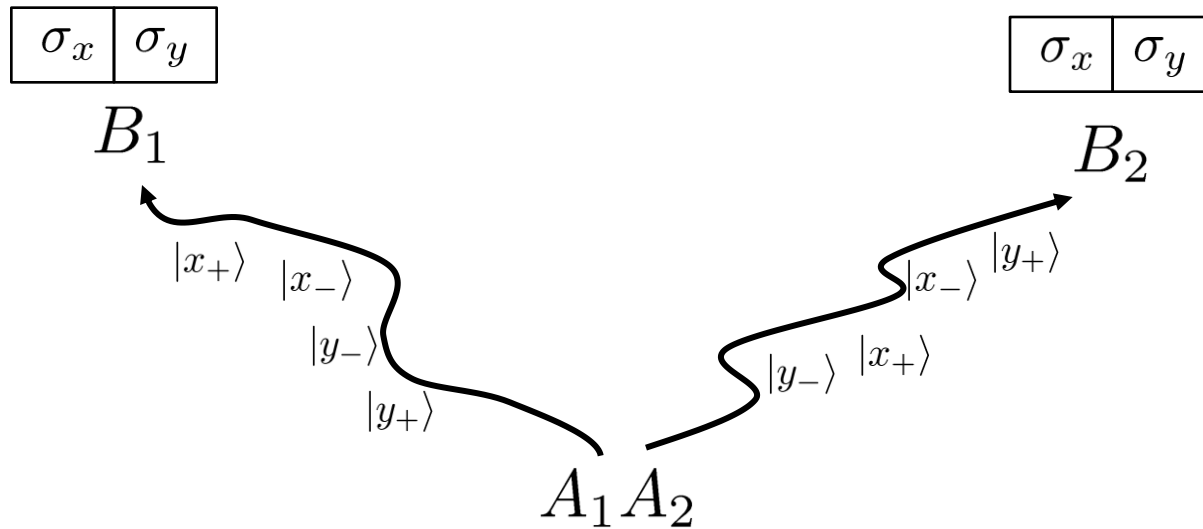**In what scenarios entanglement can improve QBER thresholds?**

Secret sharing

A wants to distribute the message to B_1, B_2 in such a way that they can learn it only if they cooperate

$$b_1 \qquad\qquad\qquad\qquad b_2$$

$$m \oplus a \oplus b_1 \oplus b_2 = m$$

$$B_1 \qquad\qquad\qquad\qquad B_2$$

$$A$$

$$m \widehat{m}\, a$$
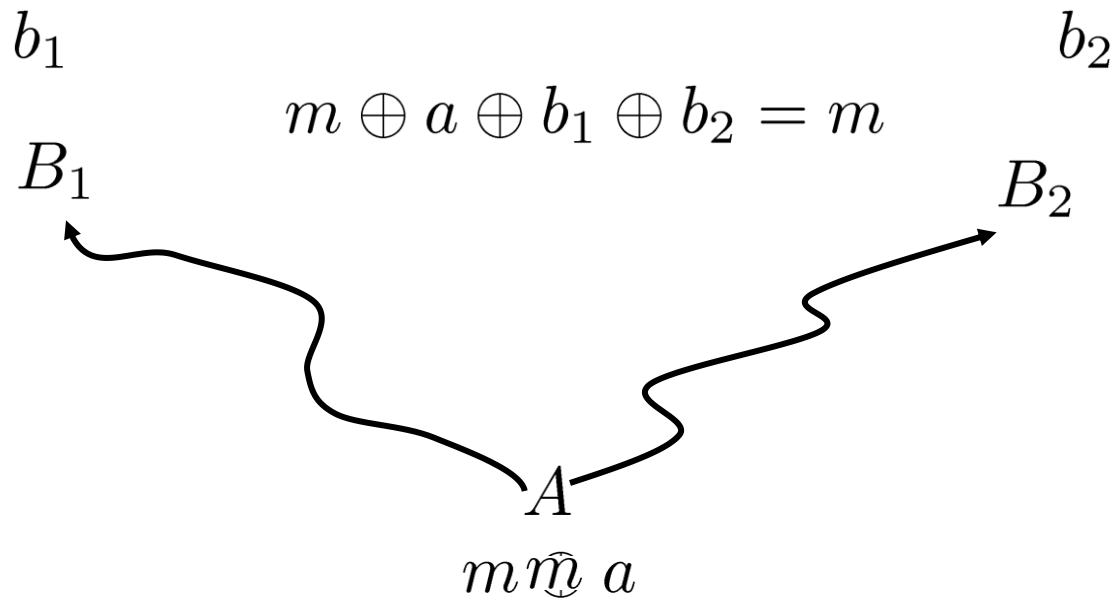
they need a random key $a \oplus b_1 \oplus b_2 = 0$

a	0		1	
b_1	0	1	0	1
b_2	0	1	1	0

Secret sharing via BB84$^{\otimes 2}$

σ_x	σ_y

B_1

σ_x	σ_y

B_2

$|x_+\rangle$ $|x_-\rangle$

$|y_-\rangle$

$|y_+\rangle$

$|x_-\rangle$ $|y_+\rangle$

$|y_-\rangle$ $|x_+\rangle$

$A_1 A_2$

A performs independent BB84 QKD with $B1$ and $B2$

$$a_1 \oplus b_1 = 0 \qquad\qquad a_2 \oplus b_1 = 0$$

$$a = a_1 \oplus a_2$$

we have the key $a \oplus b_1 \oplus b_2 = 0$

Secret sharing using GHZ
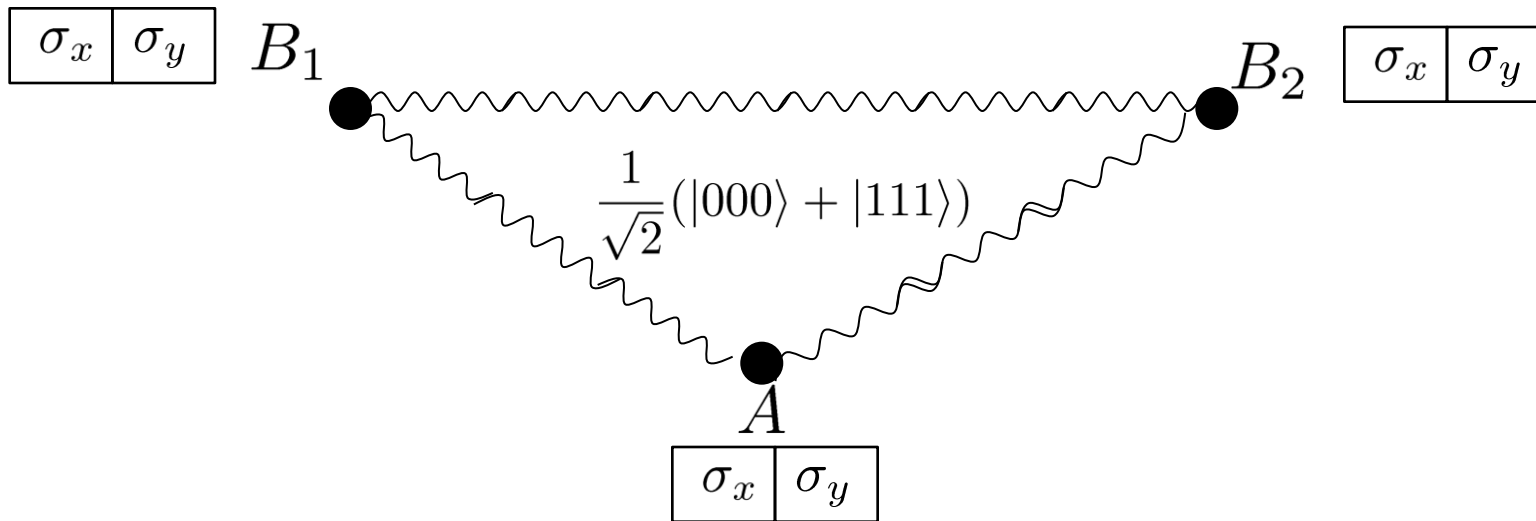
A, $B1$, $B2$ randomly measure in σ_x or σ_y eigenbasis.

$$\langle \sigma_x \otimes \sigma_x \otimes \sigma_x \rangle = 1 \qquad\qquad \langle \sigma_x \otimes \sigma_x \otimes \sigma_y \rangle = 0$$

$$\langle \sigma_x \otimes \sigma_y \otimes \sigma_y \rangle = -1 \qquad\qquad \langle \sigma_x \otimes \sigma_y \otimes \sigma_x \rangle = 0$$

$$\langle \sigma_y \otimes \sigma_x \otimes \sigma_y \rangle = -1 \qquad\qquad \langle \sigma_y \otimes \sigma_x \otimes \sigma_x \rangle = 0$$
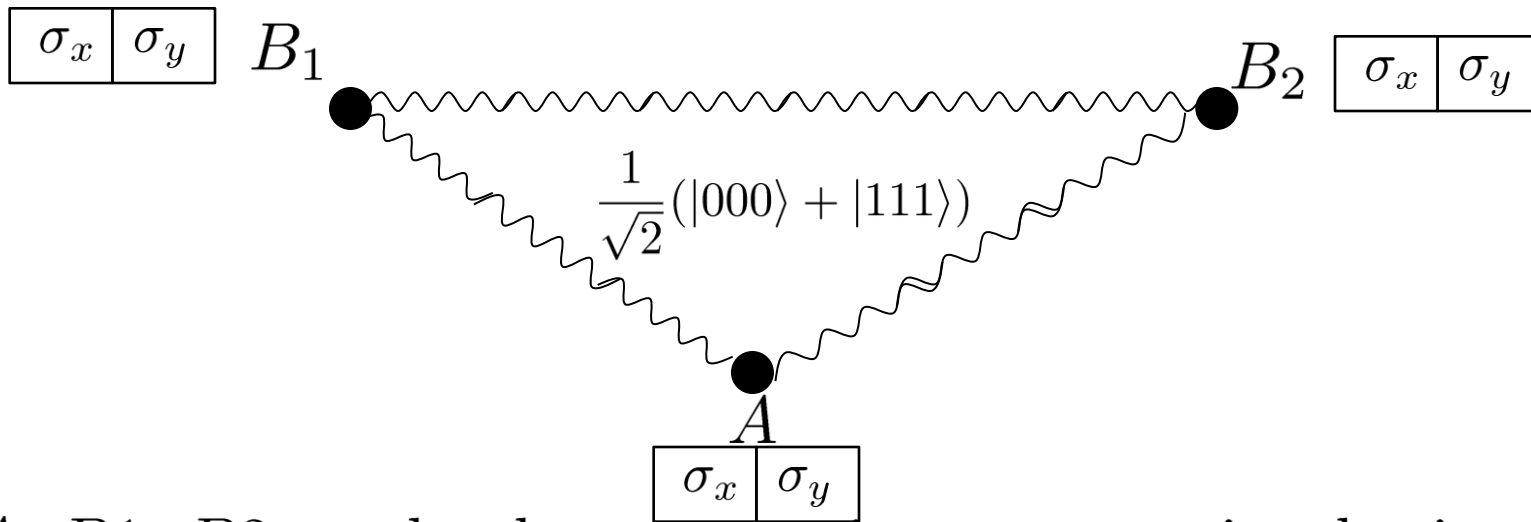
$$\langle \sigma_y \otimes \sigma_y \otimes \sigma_x \rangle = -1 \qquad\qquad \langle \sigma_y \otimes \sigma_y \otimes \sigma_y \rangle = 0$$

Secret sharing using GHZ

Proof of security via distilation: *K. Chen, H. K. Lo, Quant. Inf. Comp. 7, 689 (2008)*

A, $B1$, $B2$ randomly measure in σ_x or σ_y eigenbasis.

$\langle \sigma_x \otimes \sigma_x \otimes \sigma_x \rangle = 1$

$\langle \sigma_x \otimes \sigma_y \otimes \sigma_y \rangle = -1$

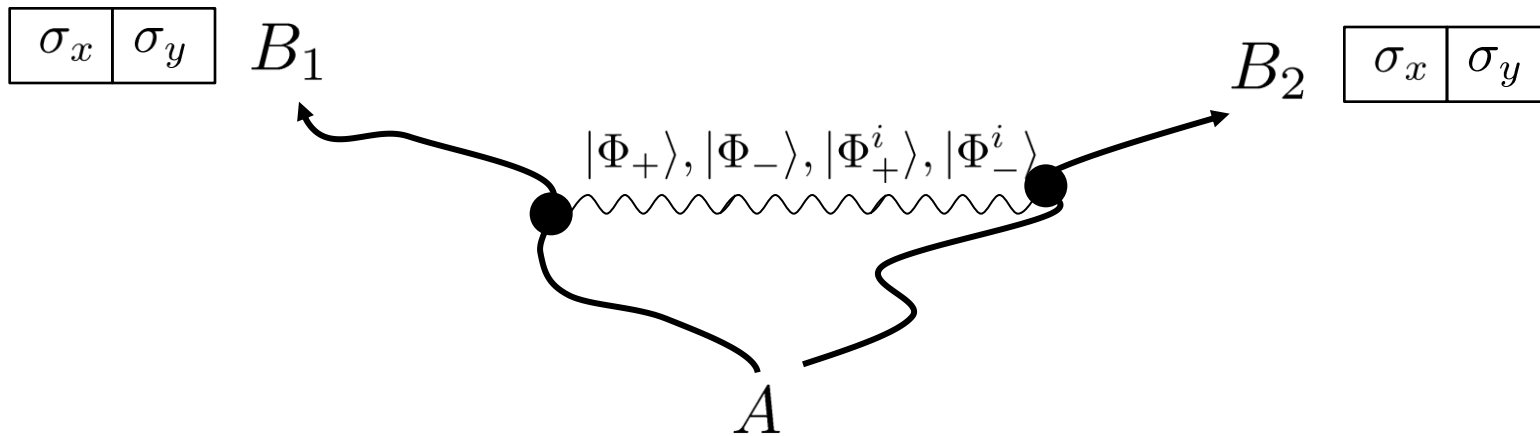$\langle \sigma_y \otimes \sigma_x \otimes \sigma_y \rangle = -1$

$\langle \sigma_y \otimes \sigma_y \otimes \sigma_x \rangle = -1$

a	0		1	
b_1	0	1	0	1
b_2	0	1	1	0

$a \oplus b_1 \oplus b_2 = 0$
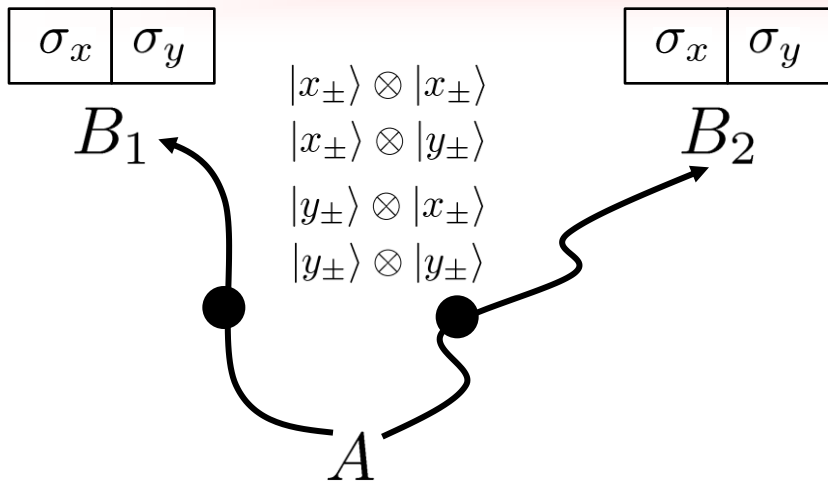
Equivalent to sending maximally entangled 2 qubit states

A sends one of four maximally entangled states to $B1$ and $B2$

base 1 $\quad |\Phi_\pm\rangle = \dfrac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \qquad \langle \sigma_x \otimes \sigma_x \rangle = \pm 1 \qquad \langle -\sigma_y \otimes \sigma_y \rangle = \pm 1$

base 2 $\quad |\Phi_\pm^i\rangle = \dfrac{1}{\sqrt{2}}(|00\rangle \pm i|11\rangle) \qquad \langle \sigma_x \otimes \sigma_y \rangle = \pm 1 \qquad \langle \sigma_y \otimes \sigma_x \rangle = \pm 1$

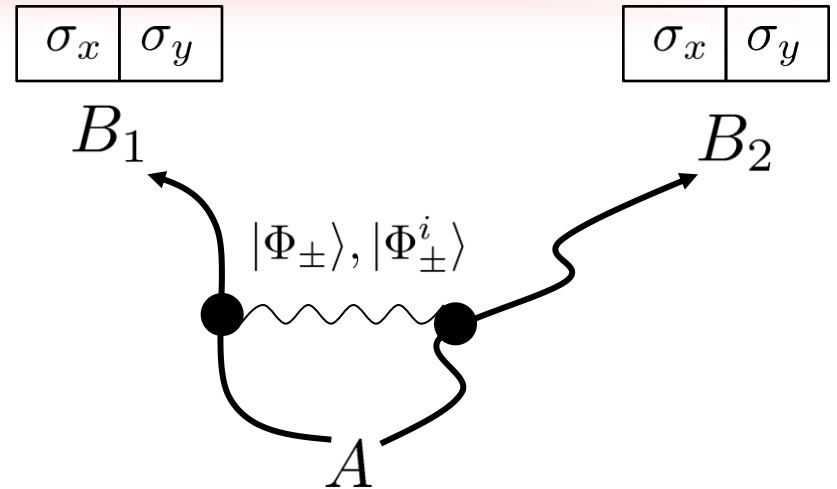**Why to use entangled states at all?**

BB84 $^{\otimes 2}$ vs. E4 protocol

$\boxed{\sigma_x \mid \sigma_y}$

$|x_\pm\rangle \otimes |x_\pm\rangle$
$|x_\pm\rangle \otimes |y_\pm\rangle$
$|y_\pm\rangle \otimes |x_\pm\rangle$
$|y_\pm\rangle \otimes |y_\pm\rangle$

B_1

$\boxed{\sigma_x \mid \sigma_y}$

B_2

A

$\boxed{\sigma_x \mid \sigma_y}$

B_1

$|\Phi_\pm\rangle, |\Phi_\pm^i\rangle$

$\boxed{\sigma_x \mid \sigma_y}$

B_2

A

error in the key when there is an error only in one channels

error $a \oplus b_1 \oplus b_2 = 1$

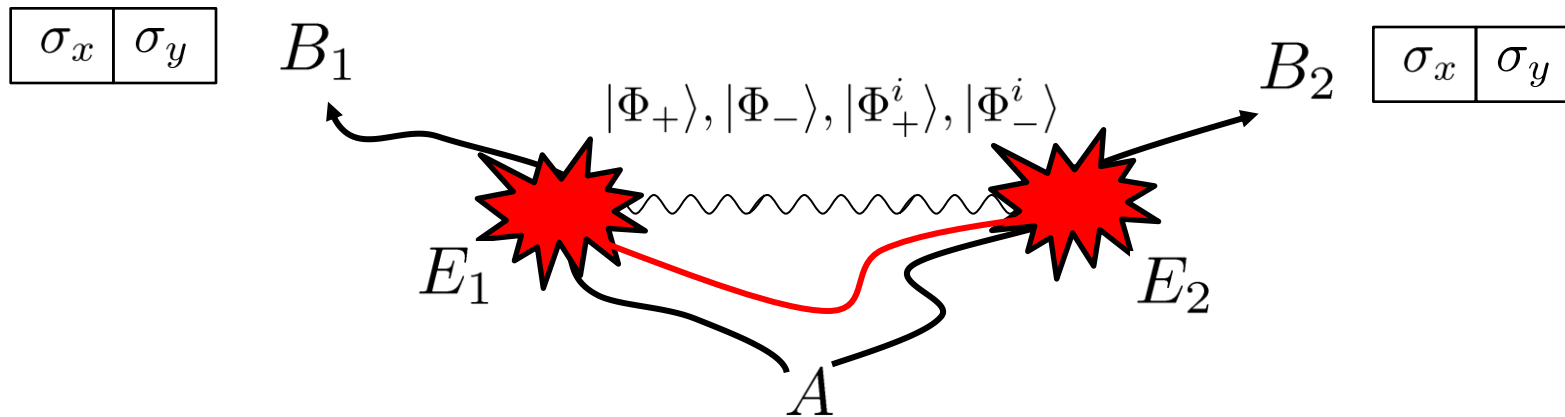$QBER_{BB84^{\otimes 2}} =$
$2QBER_{BB84}(1 - QBER_{BB84}) = 25\%$

equivalent to a single BB84

j	$|\Phi^{j,0}\rangle$	$|\Phi^{j,1}\rangle$	measurements
1	$|\Phi_+\rangle$	$|\Phi_-\rangle$	$\sigma_x \otimes \sigma_x, \ -\sigma_y \otimes \sigma_y$
2	$|\Phi_+^i\rangle$	$|\Phi_-^i\rangle$	$\sigma_x \otimes \sigma_y, \ \ \ \sigma_y \otimes \sigma_x,$

$QBER_{E4} = \dfrac{1 - 1/\sqrt{2}}{2} \approx 14.6\%$

Entanglement is irrelevant in such setup

LOCC individual attacks without quantum memory

σ_x | σ_y

B_1

$|\Phi_+\rangle, |\Phi_-\rangle, |\Phi_+^i\rangle, |\Phi_-^i\rangle$

B_2 | σ_x | σ_y
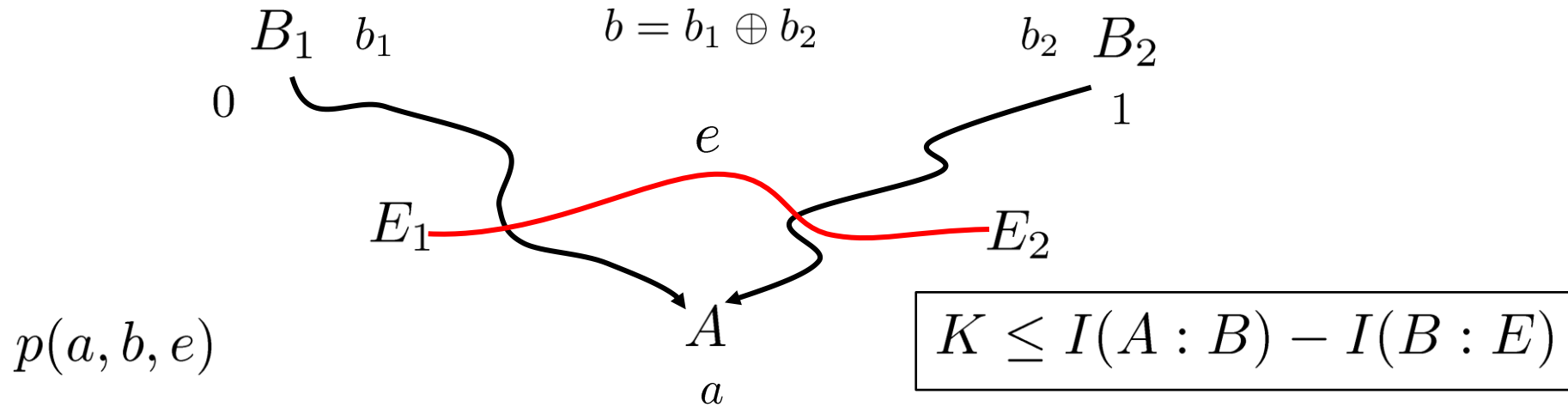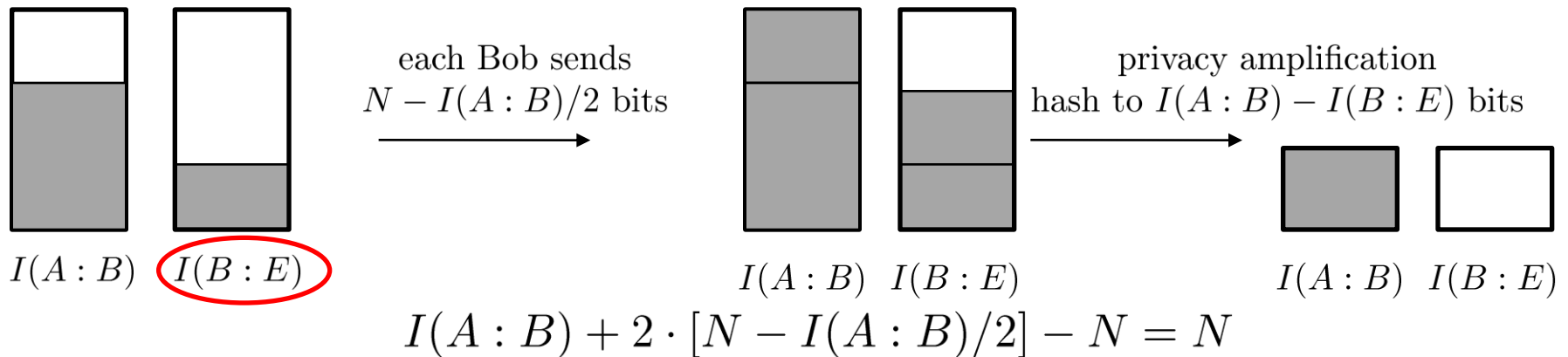
E_1

E_2

A

Motivation

- realistic assumptions on eavesdropper $\rightarrow$ higher QBER

- in secret sharing 2 channels are remote – hard to access coherently

- individual attacks in secret sharing $\rightarrow$ individual LOCC attacks

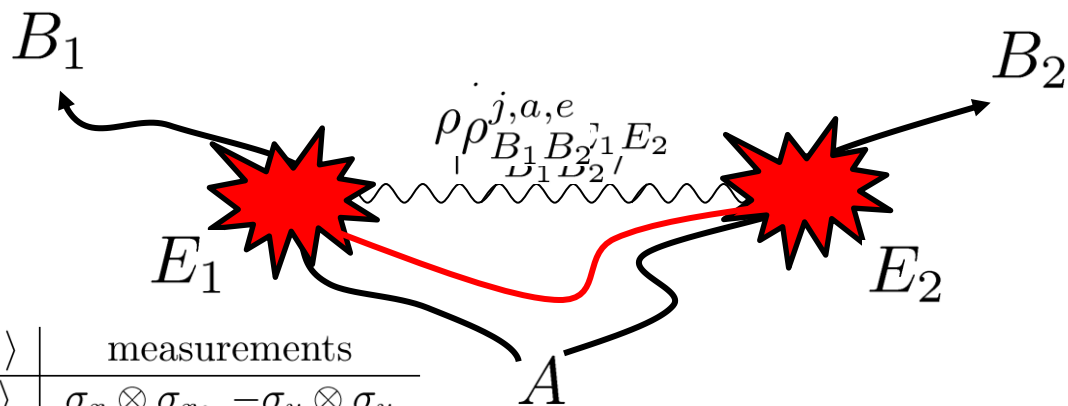**Find any advantage of using entangled states in cryptography!**

Error correction + privacy amplification in secret sharing

$$B_1 \quad b_1 \qquad\qquad b = b_1 \oplus b_2 \qquad\qquad b_2 \quad B_2$$

0

e

1

$E_1 \qquad\qquad\qquad\qquad\qquad\qquad E_2$

$p(a, b, e)$

A

a

$$\boxed{K \leq I(A:B) - I(B:E)}$$

Error correction can be done only from B_1, B_2 to A

each Bob sends
$N - I(A:B)/2$ bits

privacy amplification
hash to $I(A:B) - I(B:E)$ bits

$I(A:B) \quad I(B:E)$

$I(A:B) \quad I(B:E)$

$I(A:B) \quad I(B:E)$

$$I(A:B) + 2 \cdot [N - I(A:B)/2] - N = N$$

LOCC individual attack

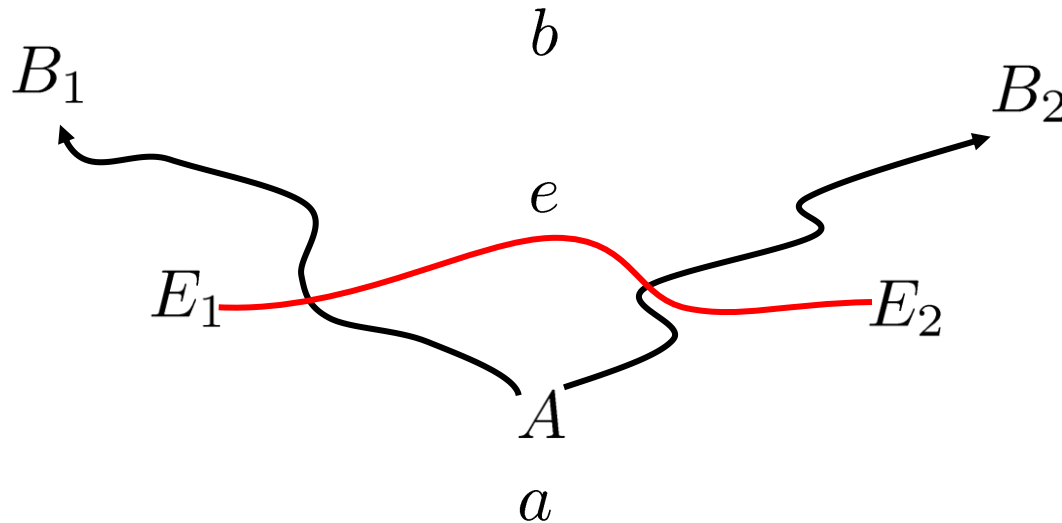| j	$\|\Phi^{j,0}\rangle$	$\|\Phi^{j,1}\rangle$	measurements
1	$\|\Phi_+\rangle$	$\|\Phi_-\rangle$	$\sigma_x \otimes \sigma_x, \ -\sigma_y \otimes \sigma_y$
2	$\|\Phi_+^i\rangle$	$\|\Phi_-^i\rangle$	$\sigma_x \otimes \sigma_y, \ \ \ \sigma_y \otimes \sigma_x,$

$e = 0, 1 - E$ information on a bit of A

$$|\Phi^{j,a}_{B_1 B_2}\rangle \overset{\mathcal{E}}{\longrightarrow} \rho^{j,a}_{B_1 B_2 E_1 E_2} \overset{\Pi^e_{E_1 E_2}}{\longrightarrow} \mathrm{Tr}_{E_1 E_2}(\rho^{j,a}_{B_1 B_2 E_1 E_2} \ \mathbb{1} \otimes \Pi^e_{E_1 E_2}) = \rho^{j,a,e}_{B_1 B_2}$$

$$\mathcal{E}^e(|\Phi^{j,a}_{B_1 B_2}\rangle\langle\Phi^{j,a}_{B_1 B_2}|) := \rho^{j,a,e}_{B_1 B_2} = \mathrm{Tr}_{E_1 E_2}(\mathcal{E}(|\Phi^{j,a}_{B_1 B_2}\rangle\langle\Phi^{j,a}_{B_1 B_2}|) \ \mathbb{1} \otimes \Pi^e_{E_1 E_2})$$

The attack is characterized by two non trace preserving CP maps
$\mathcal{E}^0, \mathcal{E}^1$ **which should be realizable by LOCC**

LOCC individual attack

$$\mathcal{E}^e(|\Phi^{j,a}_{B_1B_2}\rangle\langle\Phi^{j,a}_{B_1B_2}|) := \rho^{j,a,e}_{B_1B_2} = \mathrm{Tr}_{E_1E_2}(\mathcal{E}(|\Phi^{j,a}_{B_1B_2}\rangle\langle\Phi^{j,a}_{B_1B_2}|)\,\mathbb{1}\otimes\Pi^e_{E_1E_2})$$

Three partite probability:

$$p_{ABE}(a,b,e) = \sum_j \frac{1}{4}\mathrm{Tr}\left[\mathcal{E}^e(|\Phi^{j,a}_{B_1B_2}\rangle\langle\Phi^{j,a}_{B_1B_2}|)\,\Pi^{j,b}_{B_1B_2}\right]^{,b}_{1B_2}\right]$$

sum over 2 basis

Bobs measurement

Optimal LOCC individual attack

$$p_{ABE}(a, b, e) = \sum_j \frac{1}{4} \text{Tr} \left[\mathcal{E}^e(|\Phi^{j,a}_{B_1 B_2}\rangle\langle\Phi^{j,a}_{B_1 B_2}|) \, \Pi^{j,b}_{B_1 B_2} \right]$$

Optmization problem

- For a given $I(A:B)$ i.e. a given $QBER = \sum_{a \neq b,e} p(a,b,e)$

- Find LOCC operations, $\mathcal{E}^0$, $\mathcal{E}^1$

- Maximizing $I(E:B)$ i.e. minimizing E error on B: $p(e \neq b) = \sum_{e \neq b,a} p(a,b,e)$

Using Choi-Jamiołkowski isomorphism

$$\mathcal{E}^0 \mapsto P_{\mathcal{E}^0}, \ \mathcal{E}^1 \mapsto P_{\mathcal{E}^1} \qquad P_{\mathcal{E}} = \mathcal{E} \otimes \mathcal{I}\left(|\Psi\rangle\langle\Psi|\right), \quad |\Psi\rangle = \sum_i |i\rangle \otimes |i\rangle$$

$$P_{\mathcal{E}} \geq 0 \quad \text{Tr}_{\text{out}} P_{\mathcal{E}} = \mathbb{1}_{\text{in}} \text{ (trace preservation)} \quad \mathcal{E}(\rho_{\text{in}}) = \text{Tr}_{\text{in}}(P_{\mathcal{E}} \, \mathbb{1}_{\text{out}} \otimes \rho_{\text{in}}^T)$$

- Imposing PPT is simple very dificult; $\qquad P_{\mathcal{E}^0}^T \geq 0, \qquad P_{\mathcal{E}^1}^T \geq 0$

M. Plenio, Phys. Rev. Lett. **95,** 090503 (2005) (monotonicity of logarithmic negativity)
RDD, A. Sen (De), U. Sen, M. Lewenstein , Phys. Rev. A, **73** 032313 (2006) (LOCC cloning of entangled states)

Optimal LOCC individual attack

$$p_{ABE}(a, b, e) = \sum_j \frac{1}{4} \mathrm{Tr}\left[P_{\mathcal{E}^e} \; \Pi_{B_1 B_2}^{j,b} \otimes |\Phi_{B_1 B_2}^{j,a}\rangle\langle\Phi_{B_1 B_2}^{j,a}|^T \right]$$

Optmization problem

- For a given $I(A:B)$ i.e. a given $QBER = \sum_{a \neq b, e} p(a, b, e)$

- Find LOCC operations, $\mathcal{E}^0$, $\mathcal{E}^1$

- Maximizing $I(E:B)$ i.e. minimizing E error on B: $p(e \neq b) = \sum_{e \neq b, a} p(a, b, e)$
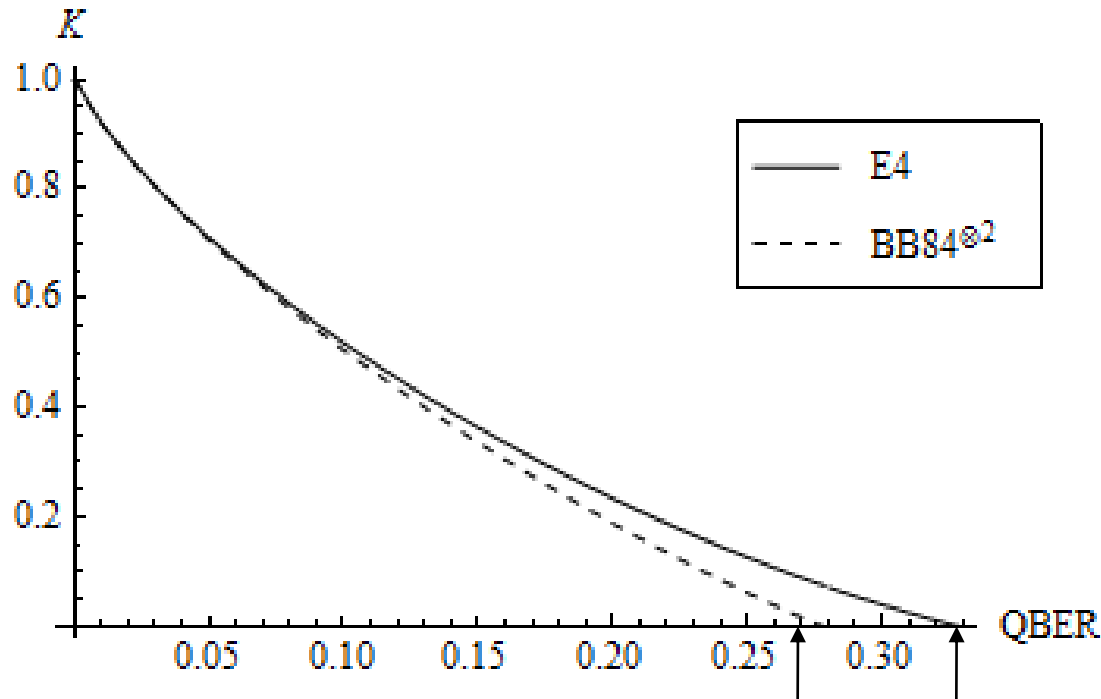
Using Choi-Jamiołkowski isomorphism

CP map condition	$P_{\mathcal{E}^0} \geq 0$	$P_{\mathcal{E}^1} \geq 0$	$\mathrm{Tr}_{\mathrm{out}}(P_{\mathcal{E}^0} + P_{\mathcal{E}^1}) = \mathbb{1}_{\mathrm{in}}$
PPT condition	$P_{\mathcal{E}^0}^T \geq 0,$	$P_{\mathcal{E}^1}^T \geq 0$	

The problem is a semi-definite program

Optimization over two, 16×16 matrices

If we explicitly show that the optimal solution is LOCC we are done!

Entangled states protocol allows for higher QBER!

- **BB84 $^{\otimes 2}$**

$QBER_{BB84^{\otimes 2}} = 5/18 \approx 27.7\%$

(without LOCC constraint: 25%)

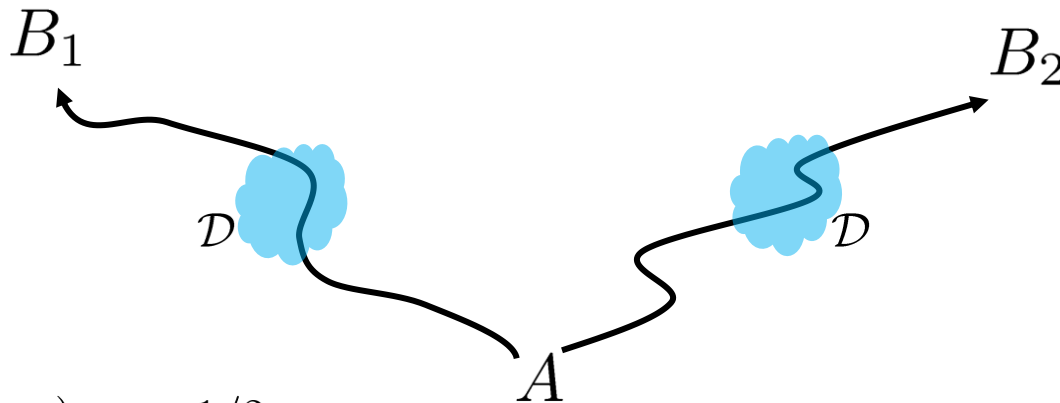requires communicating 2 bits

- **E4**

$QBER_{E4} = 2(\sqrt{2} - 5/4) \approx 32.8\%$

(without LOCC constraint: $14,6\%$)

requires communicating $\log_2 27$ bits

Practical application
two independent isotropically depolarizing channels

$$\mathcal{D}(\rho) = (1 - \alpha)\rho + \alpha \mathbb{1}/2$$

Under the action of $\mathcal{D}^{\otimes 2}$, $QBER = \alpha(1 - \alpha/2)$ in both $BB84^{\otimes 2}$ and $E4^{\otimes 2}$

We can perform secret sharing via E4 using more noisy channels

- **BB84$^{\otimes 2}$**

$QBER_{BB84^{\otimes 2}} = 5/18 \approx 27.7\%$

(without LOCC constraint: 25%)

requires communicating 2 bits

- **E4**

$QBER_{E4} = 2(\sqrt{2} - 5/4) \approx 32.8\%$

(without LOCC constraint: $14, 6\%$)

requires communicating $\log_2 27$ bits

Summary

- **Without imposing LOCC constraints on eavesdropper, entangled states are useless in secret sharing**

- **If LOCC condtion is imposed, and individual attack scenario considered, entagled states offer higher tolerable QBER**

$$QBER_{BB84^{\otimes 2}} = 5/18 \approx 27.7\% \qquad QBER_{E4} = 2(\sqrt{2} - 5/4) \approx 32.8\%$$

- **One way error-correction can be perfomed only from B1,B2 $\rightarrow$ A, which leads to a simplified Csiszar-Koerner theorem**

- **Another example of strength of PPT condition when looking for optimal LOCC operations**

- **Open problems:**

- secret sharing protocols yielding highest QBER under individual LOCC attacks
- relation with LOCC distinguishability of entangled states