Entanglement enhances security in secret sharing

Rafał Demkowicz-Dobrzański

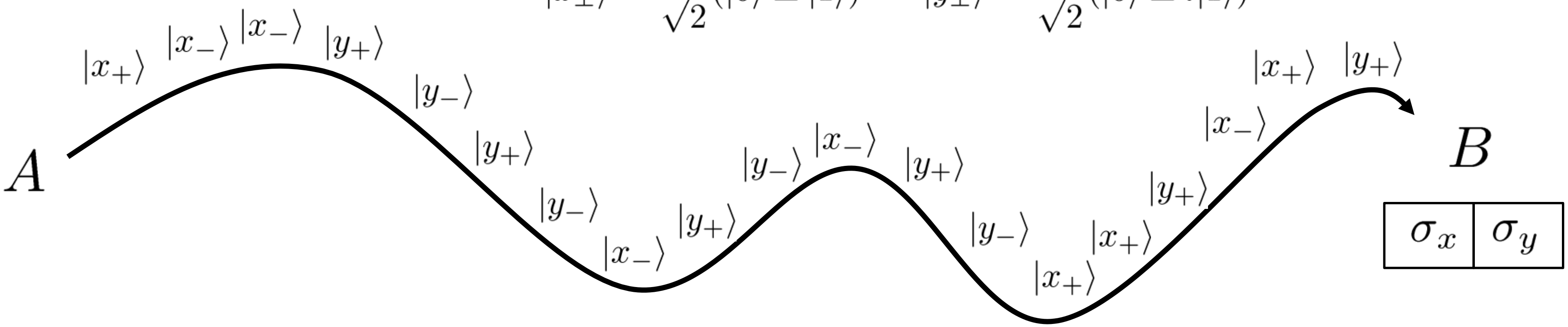
Nicolaus Copernicus University, Toruń, Poland

Aditi Sen (De), Ujjwal Sen, Maciej Lewnestein

ICFO-Institut de Ciencies Fotoniques, Barcelona, Spain

Quantum Key Distribution

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

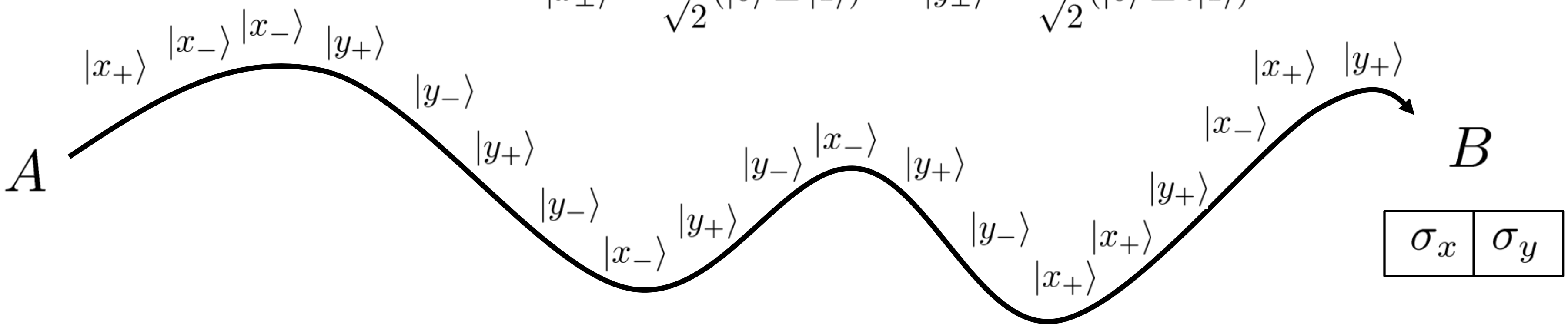


BB84 protocol

A key	0	0	0	1	1	1	0	0	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	0	?	?	1	?	?	0	?	0

Quantum Key Distribution

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



Sifting phase

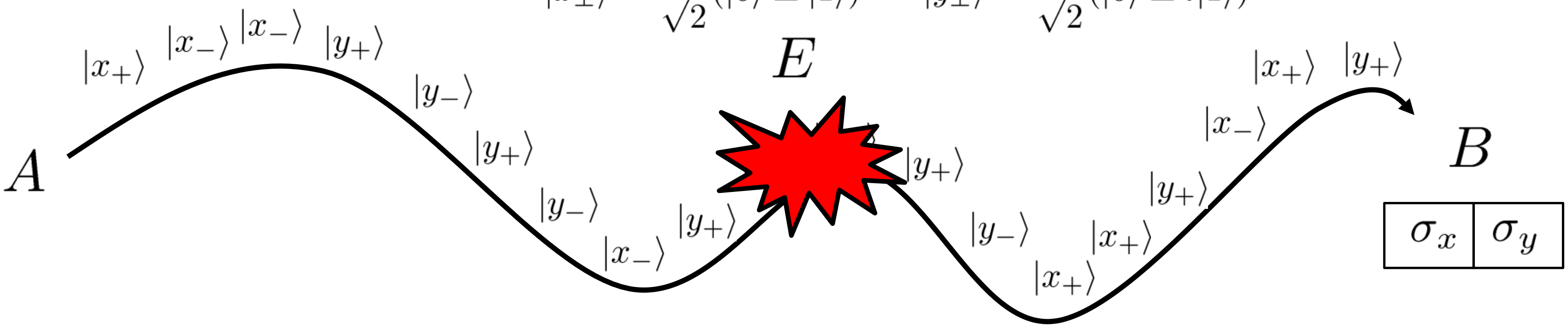
A key	0	0			1			0		0
A	x_+	y_+	y_+	y_-	x_-	x_-	x_+	y_+	y_+	x_+
B	σ_x	σ_y	σ_x	σ_x	σ_x	σ_y	σ_y	σ_y	σ_x	σ_x
compatible?	✓	✓			✓			✓		✓
B key	0	0			1			0		0

a random key $a \oplus b = 0$

encryption $m \oplus a \longrightarrow m \oplus a \oplus b = m$ decryption

Quantum Key Distribution

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



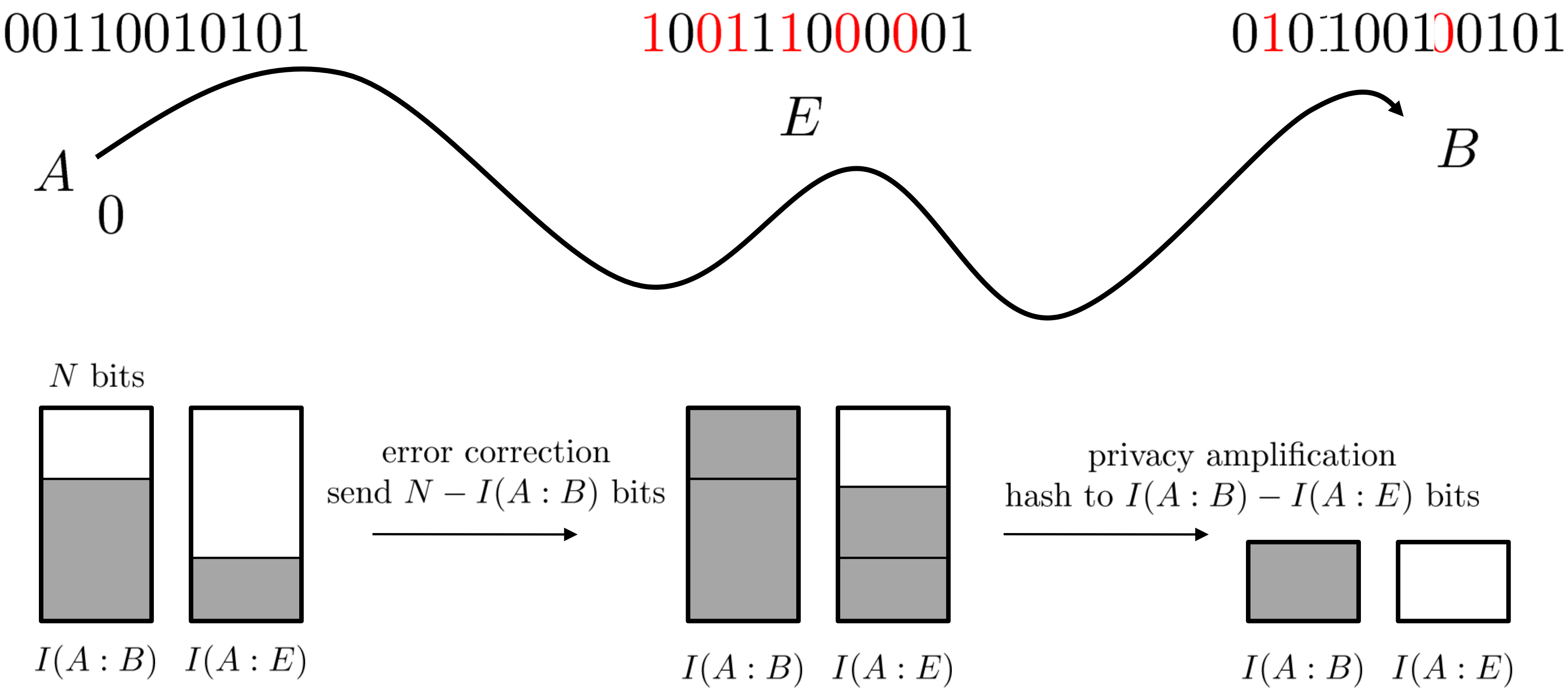
In reality there are errors

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

Reveal part of bits to estimate QBER

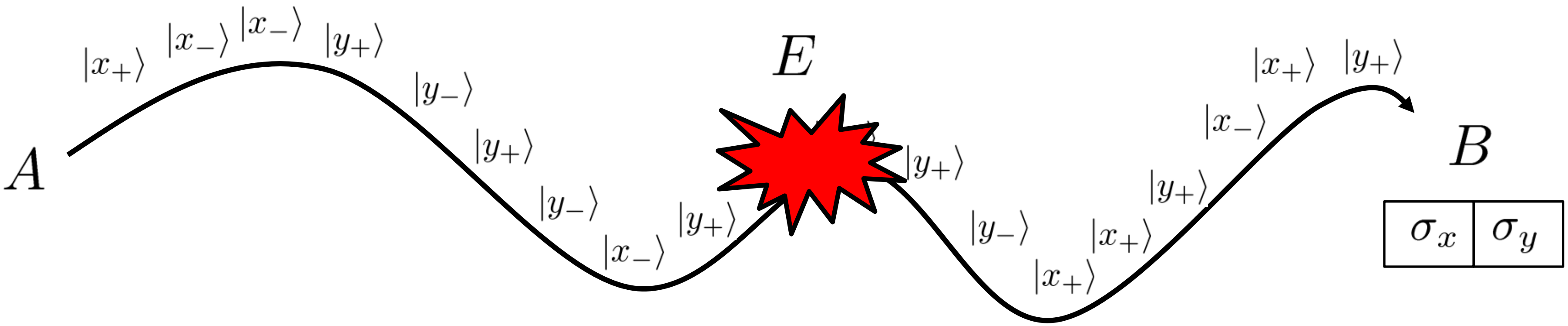
If low enough, perform error-correction + privacy amplification

Error correction + privacy amplification



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

Key genration rate in QKD



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

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

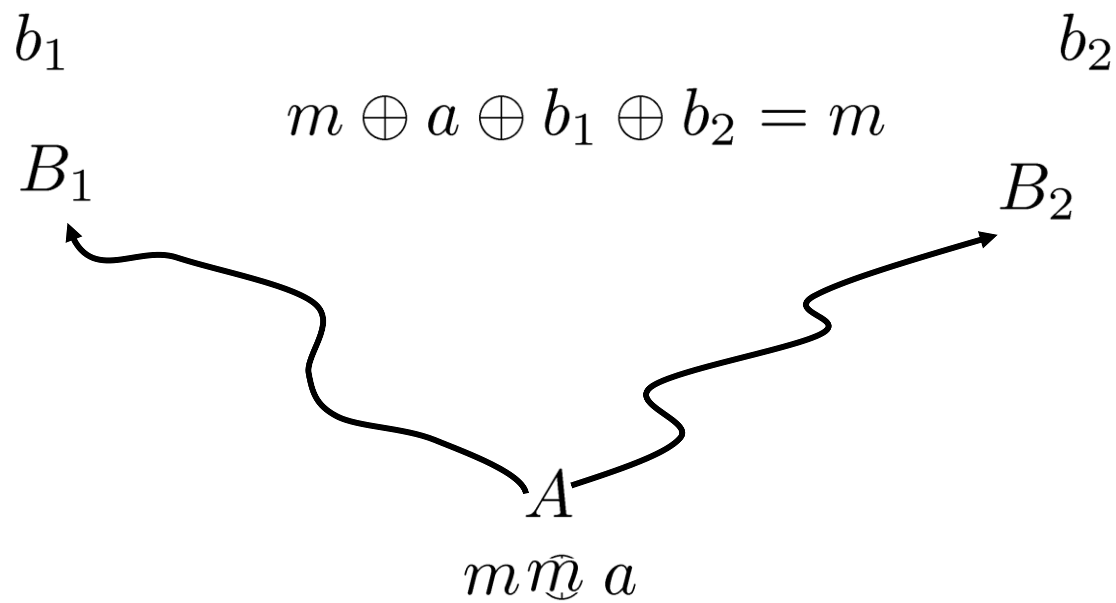
QBER threshold for BB84:

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

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

Secret sharing

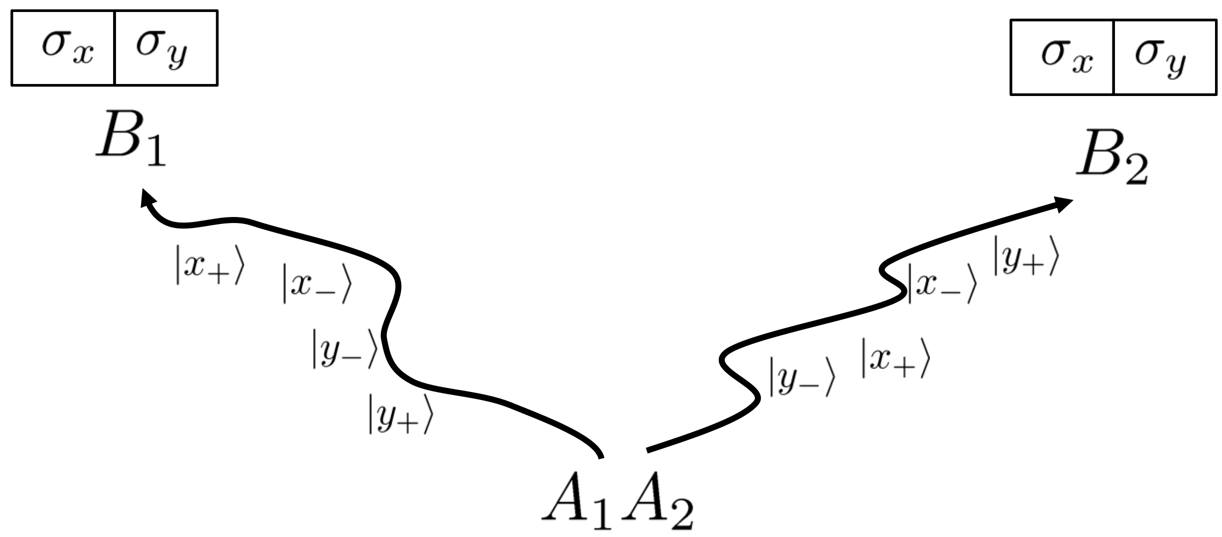
A **wants to distribute the message to** $\boldsymbol{B_1}$**,** $\boldsymbol{B_2}$ **in such a way that they can learn it only if they cooperate**



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$^{\otimes 2}$



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

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

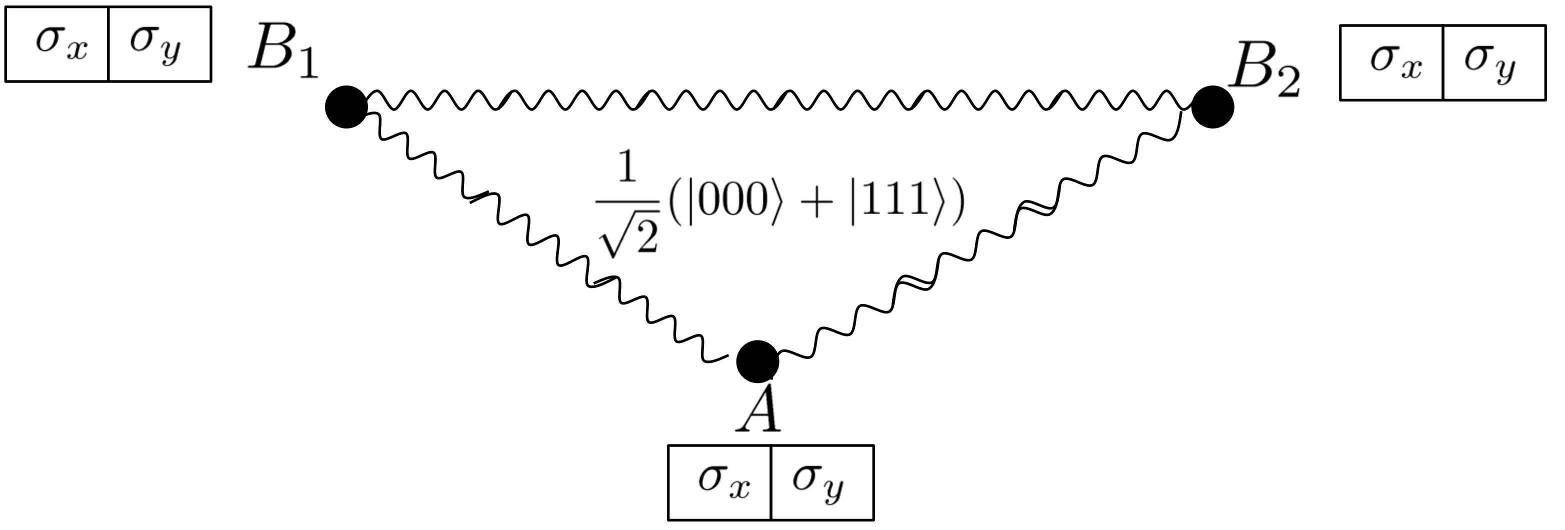
$$a = a_1 \oplus a_2$$

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

Secret sharing using GHZ

M. Żukowski, et al. Acta Phys. Pol. 93, 187 (1998)

M. Hillery, V. Buzek, A. Berthiaume, Phys. Rev. A 59, 1829 (1999)



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

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

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

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

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

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

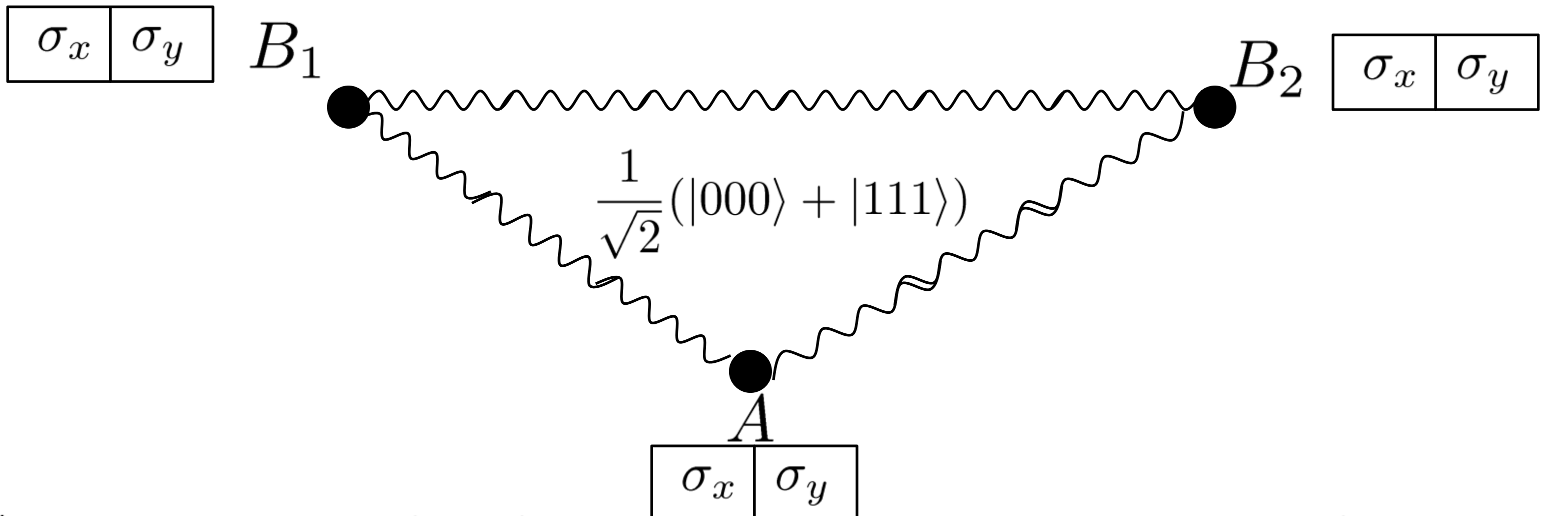
$$\langle \sigma_x \otimes \sigma_y \otimes \sigma_x \rangle = 0$$

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

$$\langle \sigma_y \otimes \sigma_y \otimes \sigma_y \rangle = 0$$

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.

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

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

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

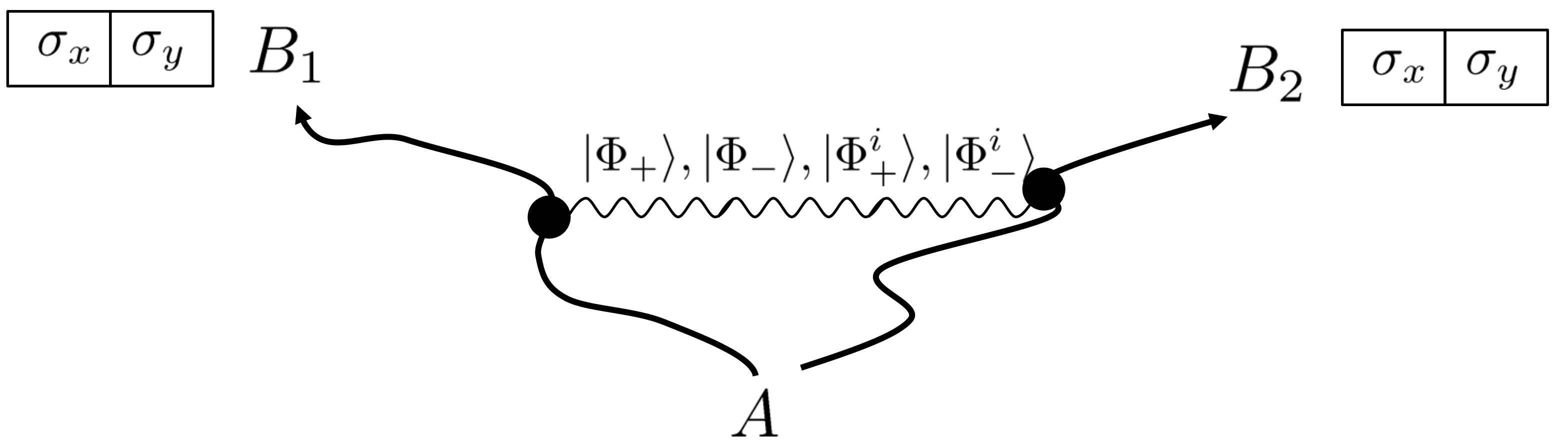
$$\langle \sigma_y \otimes \sigma_y \otimes \sigma_x \rangle = -1$$

$\longrightarrow$

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



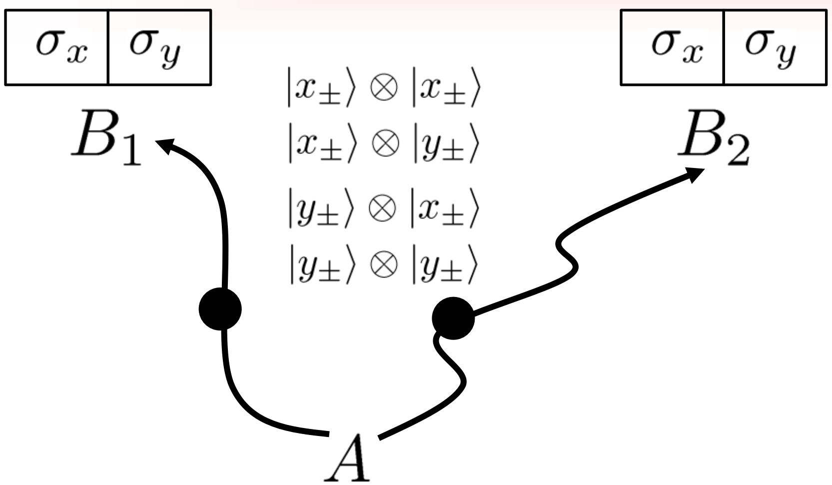
A sends one of four maximally entangled states to $B1$ and $B2$

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

base 2 $\quad |\Phi^i_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm i|11\rangle) \quad \langle \sigma_x \otimes \sigma_y \rangle = \pm 1 \quad \langle \sigma_y \otimes \sigma_x \rangle = \pm 1$

Why to use entangled states at all?

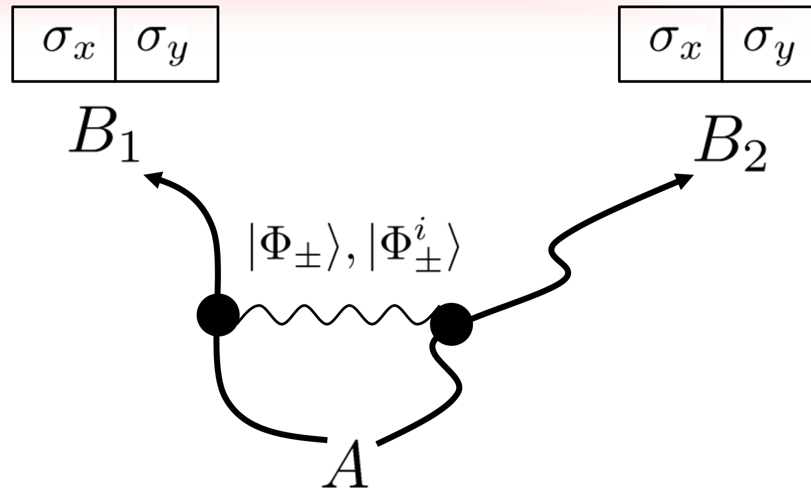
BB84$^{\otimes 2}$ vs. E4 protocol



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

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

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



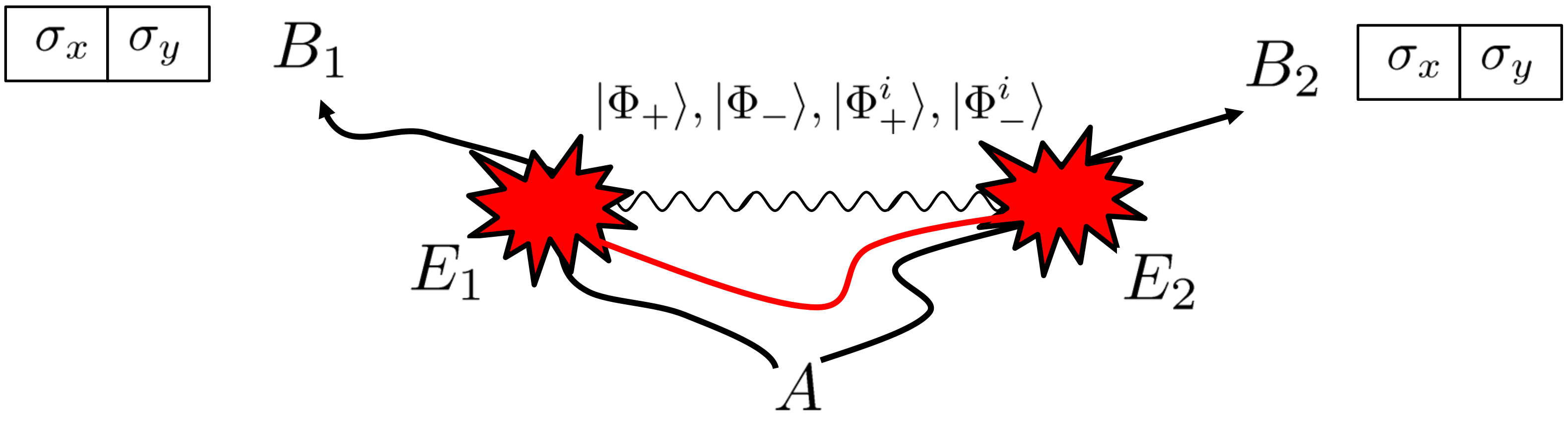
equivalent to a single BB84

j	$\lvert\Phi^{j,0}\rangle$	$\lvert\Phi^{j,1}\rangle$	measurements
1	$\lvert\Phi_+\rangle$	$\lvert\Phi_-\rangle$	$\sigma_x \otimes \sigma_x, \quad -\sigma_y \otimes \sigma_y$
2	$\lvert\Phi^i_+\rangle$	$\lvert\Phi^i_-\rangle$	$\sigma_x \otimes \sigma_y, \quad \sigma_y \otimes \sigma_x,$

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

Entanglement is irrelevant in such setup

LOCC individual attacks without quantum memory

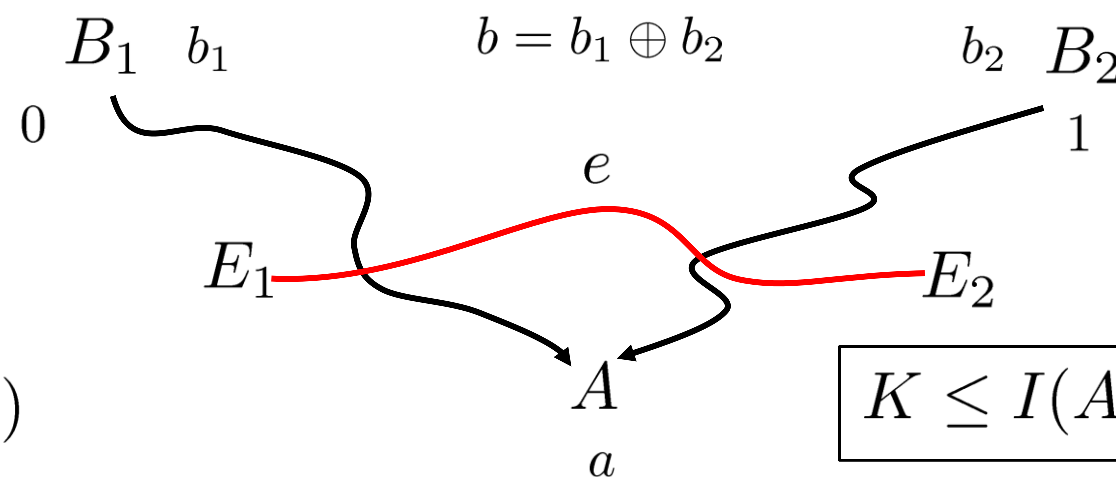


Motivation

- 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!

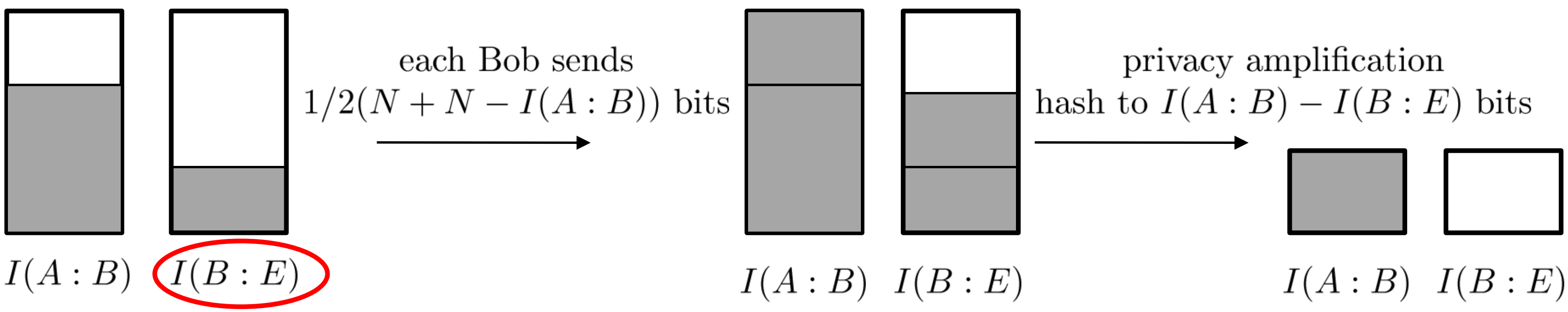
Error correction + privacy amplification in secret sharing



$p(a, b, e)$

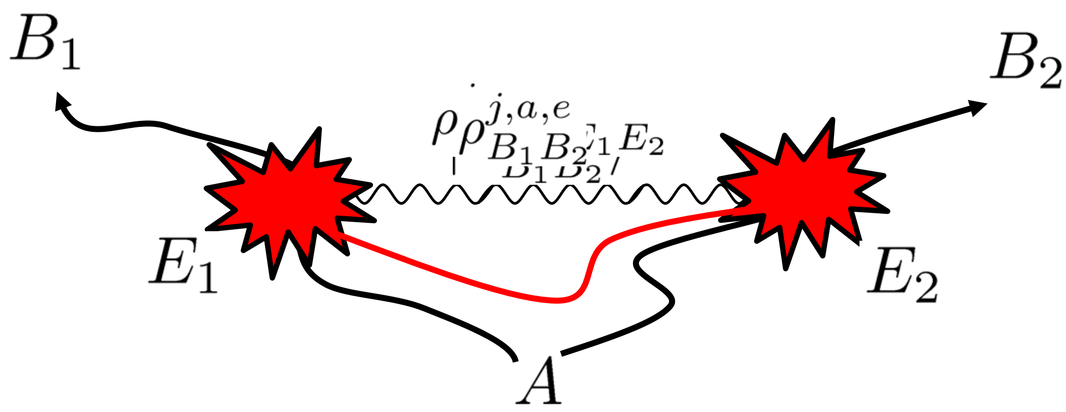
$$\boxed{K \leq I(A:B) - I(B:E)}$$

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



$$I(A:B) + 2 \cdot \frac{1}{2}\left[N + N - I(A:B)\right] - N = N$$

LOCC individual attack



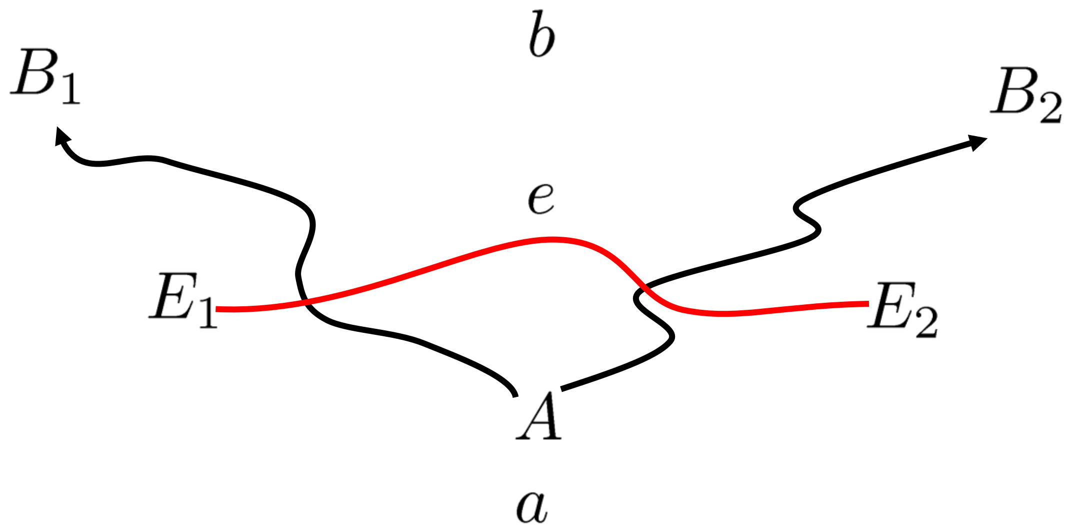
$e = 0, 1$ – E information on a bit of A

$$|\Phi^{j,a}_{B_1B_2}\rangle \xrightarrow{\mathcal{E}} \rho^{j,a}_{B_1B_2E_1E_2} \xrightarrow{\Pi^e_{E_1E_2}} \mathrm{Tr}_{E_1E_2}(\rho^{j,a}_{B_1B_2E_1E_2}\; \mathbb{1}\otimes\Pi^e_{E_1E_2}) = \rho^{j,a,e}_{B_1B_2}$$

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

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:

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

sum over 2 basis

Bobs measurement

Optimal LOCC individual attack

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

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

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

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

- Imposing PPT is simple very dificult $\qquad P^T_{\mathcal{E}^0} \geq 0, \qquad P^T_{\mathcal{E}^1} \geq 0$

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

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

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

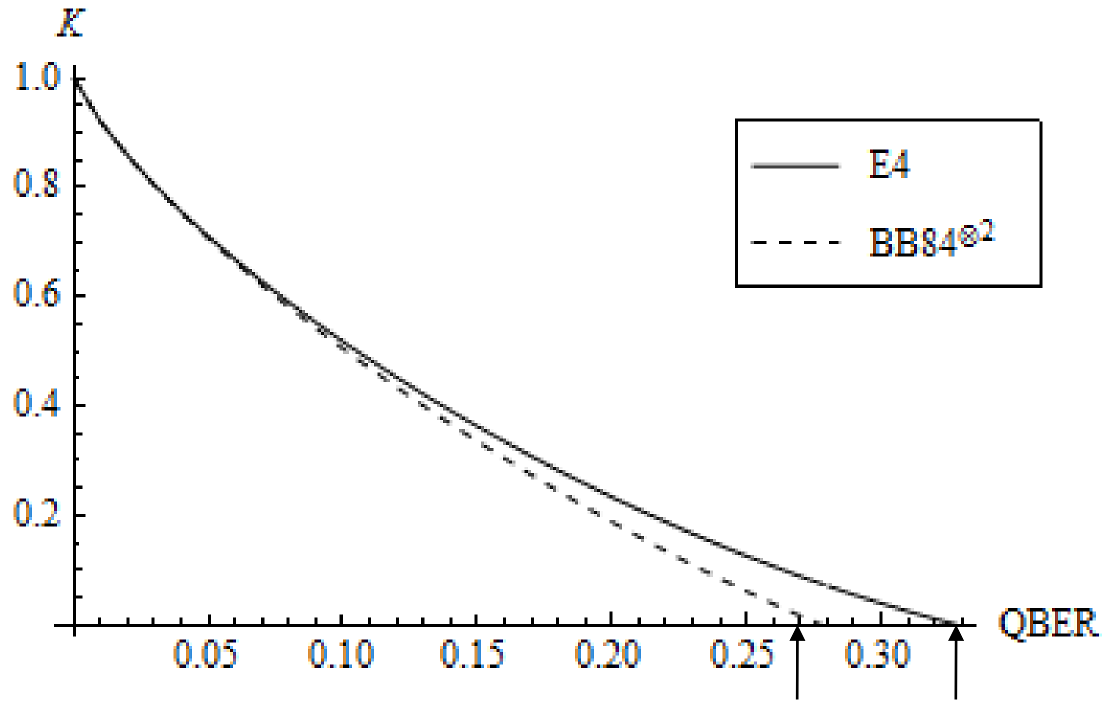
CP map condition	$P_{\mathcal{E}^0} \geq 0$	$P_{\mathcal{E}^1} \geq 0$	$\mathrm{Tr}_{\mathrm{out}}(P_{\mathcal{E}^0} + P_{\mathcal{E}^1}) = \mathbb{1}_{\mathrm{in}}$
PPT condition	$P^T_{\mathcal{E}^0} \geq 0,$	$P^T_{\mathcal{E}^1} \geq 0$	

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**

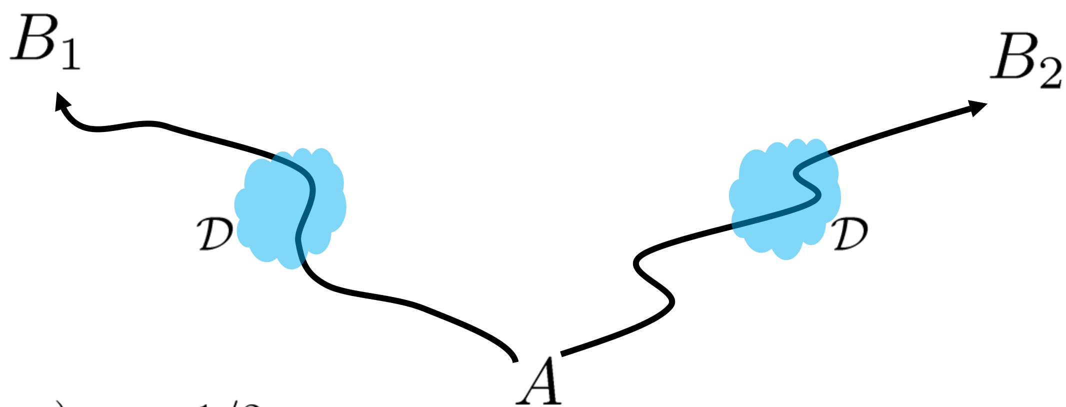
$$QBER_{E4} = 2(\sqrt{2} - 5/4) \approx 32.8\%$$

(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, entagled 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 → 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

R. Demkowicz-Dobrzański, A. Sen (De), U. Sen, M. Lewenstein , arxiv:0802.1811