Upper bounds on secret key rate in various quantum and beyond-quantum cryptographic scenarios

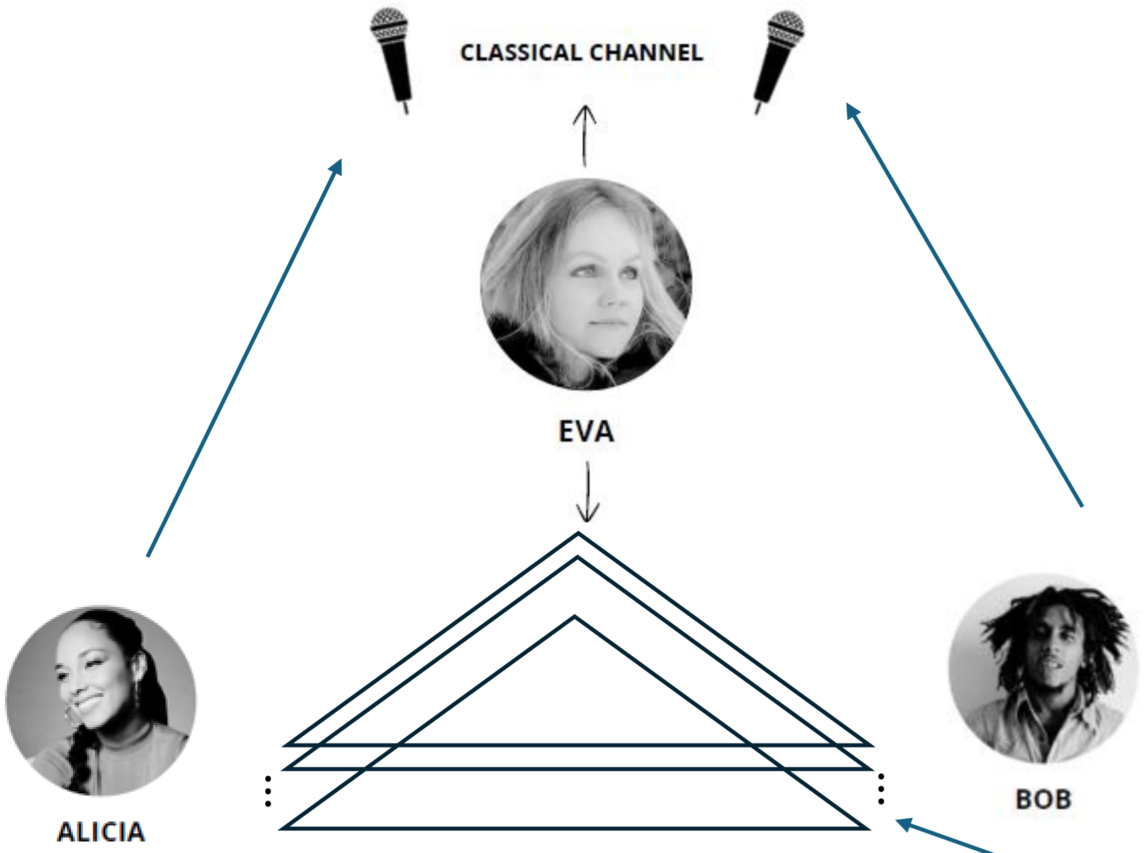
Karol Horodecki
Division of Quantum Information, Institute of Informatics
University of Gdańsk

International Symposium on Quantum Information and Quantum Communication
Centre for Quantum Engineering , Research and Education (CQuERE), TCG CREST
Kolkata 2.04. 2025

University of Gdańsk

NATIONAL SCIENCE CENTRE
POLAND

Secret key distribution scenario and distillable secret key



Secret key : random bitstring known only to Alice and Bob
Task: distribute secret key

n shared tripartite „objects”

$$distillable\ secret\ key(\text{object}) = \sup_{Protocol \in allowed\ operations} \left\{ \frac{k}{n} : Protocol(n\ "objects") \approx_{\epsilon} secret\ key\ of\ length\ k \right\}$$

$$(for\ large\ n\ and\ small\ \epsilon)$$

Various quantum key distribution scenarios

Increasing level of professional paranoia

$(\rho, \mathcal{M})$

$(\rho, \mathcal{M})?$

$?$

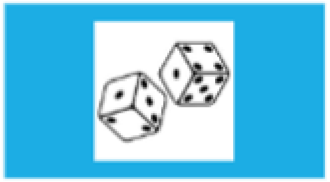
Classical Secure Key Agreement Scenario (SKA)

Device Dependent quantum cryptography (DD)

Device Independent quantum cryptography (DI)

Non-signaling Device Independent cryptography (NSDI)

Secure key agreement

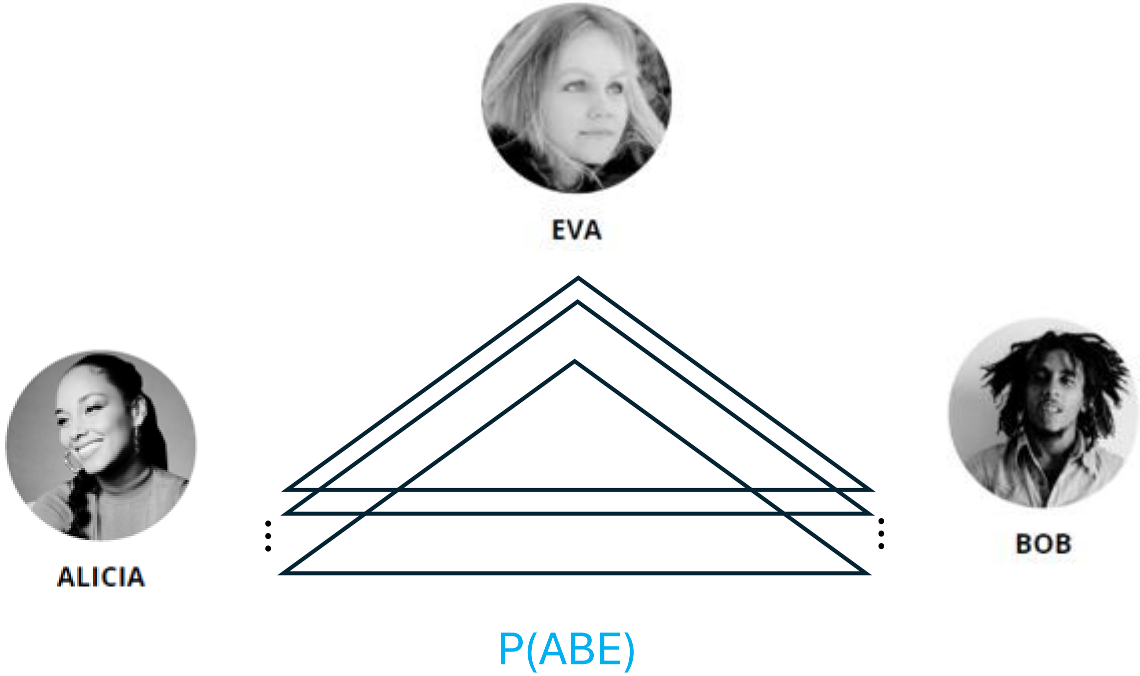


Shared objects: triples of random variables A,B,E with distribution P(ABE)

Allowed operations: Local Classical Operations and Public Communication

Trust: honest parties share P(AB) and Eve knows only E with total P(ABE) distribution about them

Resource:
Partially secret correlations



K_{SKA} $-$ *distilable key*

Quantum device dependent scenario

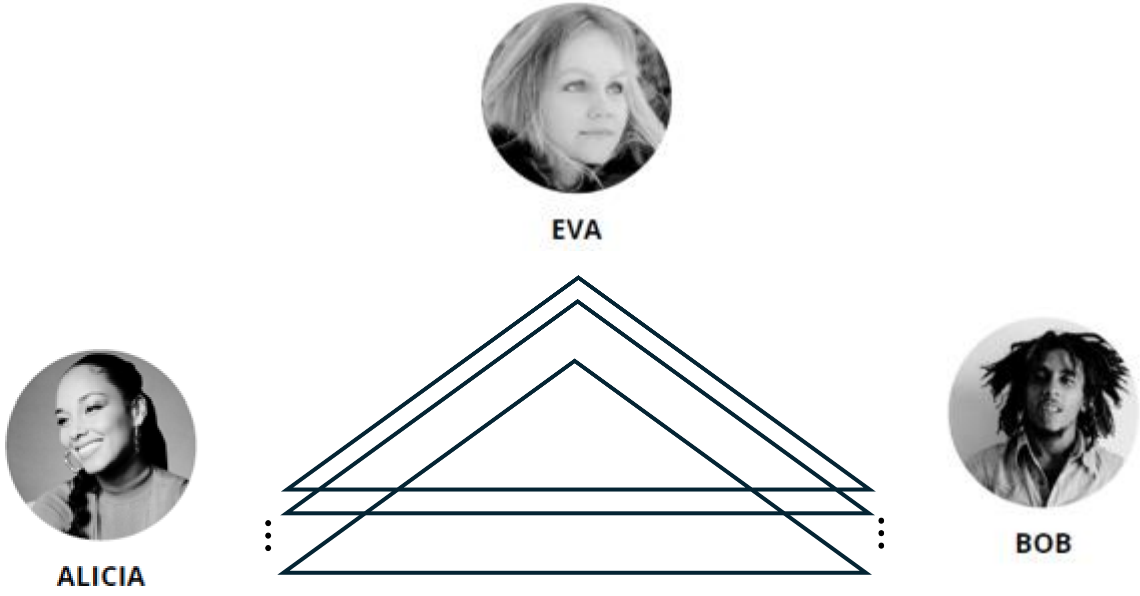
$(\rho, \mathcal{M})$

Shared objects: tripartite quantum pure states: $|\psi_{ABE}\rangle$

Allowed operations: Local Quantum Operations and Classical Communication (LOCC)

Trust: dimension of the input state ρ in Alice's and Bob's hands, and quantum operations they use

Resource:
Quantum Entanglement



$|\psi_{ABE}\rangle$

K_{DD} $-$ *device dependent distilable key*

Device independent scenario

$(\rho, \mathcal{M})?$

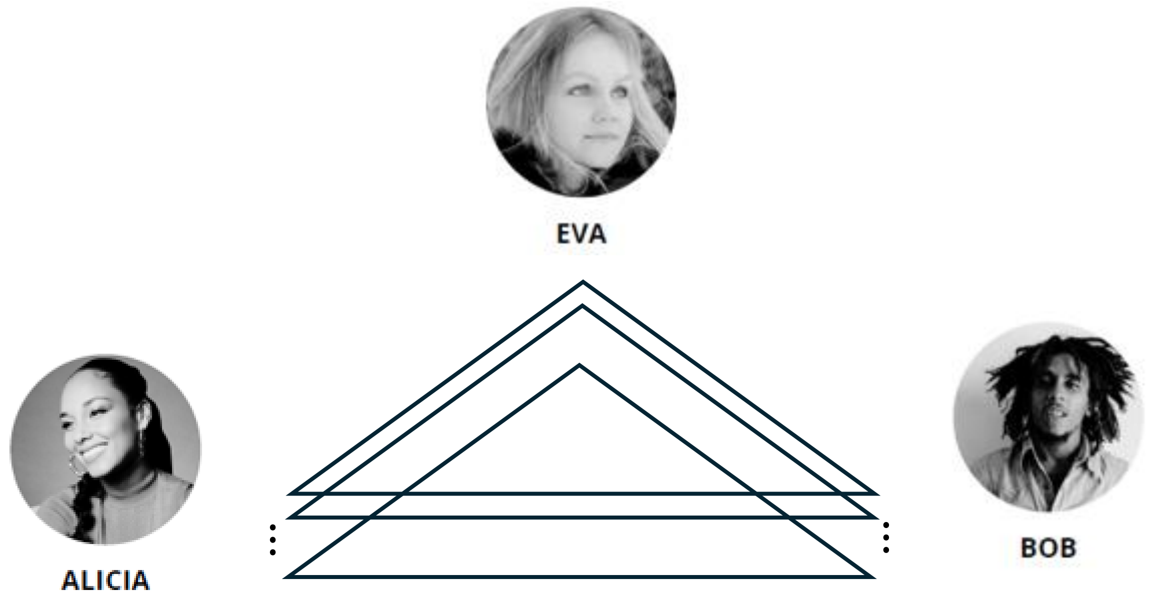
Shared objects: quantum extensions of conditional probability distributions

Alice & Bob have : P(ab|xy)=$Tr M_a^x \otimes M_b^y \otimes I_E |\psi_{ABE}\rangle\langle\psi_{ABE}|$, Eve holds purifying system E

Allowed operations: Local classical operations and Public Communication (cLOPC)

- **Trust:** Quantum, but untrusted device
- Possible attack e.g. $N_a^x \otimes N_b^y$ and σ_{AB} such that $(\mathrm{N}, \sigma) \equiv Tr\, N_a^x \otimes N_b^y \sigma_{AB} = Tr\, M_a^x \otimes M_b^y \rho_{AB} \equiv (\rho, M)$

Resource:
Bell non-locality



$\{\mathrm{P(ab|xy)}\rho_E^{xyab}\}$

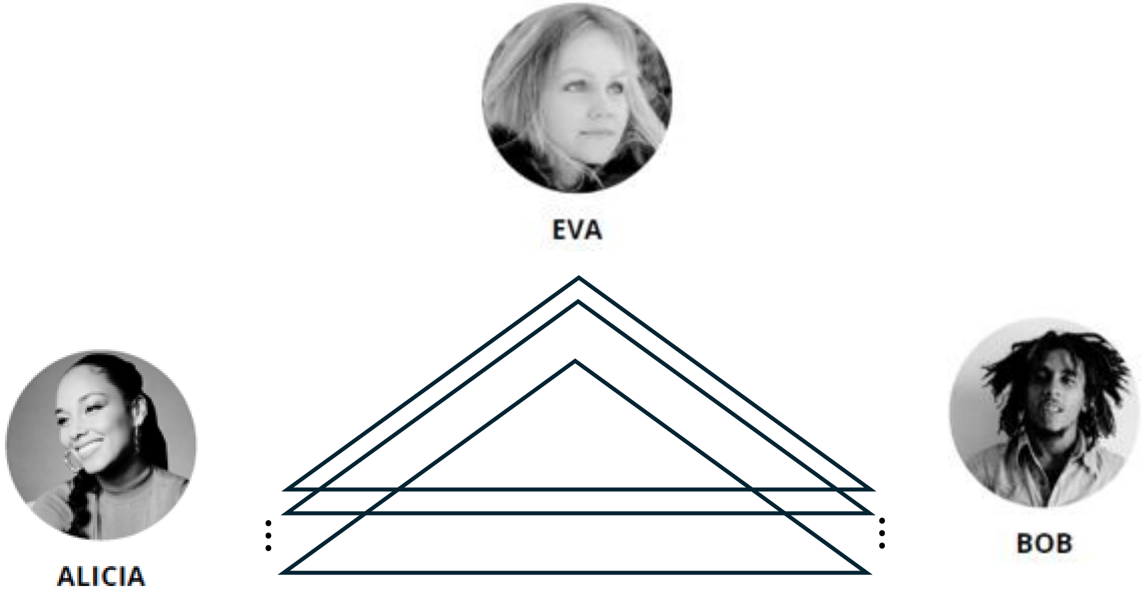
K_{DI} $-$ *device independent distilable key*

non-signaling device independent scenario

Shared objects: conditional probability distributions P(abe|xyz)
Allowed operations: Direct measurements +Local **classical** operations and Public Communication (DcLOPC)

Unknown physics of the device P(ab|xy)
Trust: device does not signal to Eve's one and vice versa (non-signaling assumption)

Resource:
Bell non-locality



P(abe|xyz)

K_{NSDI} $- non - signaling$ $device\ independent$ $distilable\ key$

Motivation & outlook

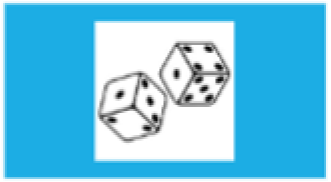
- Lower bounds on secret key as achieved by found protocols
  e.g. BB84 are well known and realized in practice
- Upper bounds can tell about optimality of these protocols

- What do we know about **upper bounds on secret key** rate
  In these scenarios ?
- Brief **overview of techniques for** constructing upper bounds on secret key

In what follows I base on the review [1] but also go beyond

[1] I.W. Primaatmaja et al. Quantum vol 7, page 932 2023

Secret Key Agreement
– bound by intrinsic information



Intrinsic information $I(A:B \downarrow E) := \inf_{\Lambda:E\to E'} I(A:B|E')$

Conditional mutual information $I(A:B|E) = H(AE) + H(BE) - H(E) - H(ABE)$

H(X) – Shannon entropy of a random variable X

$$I(A:B \downarrow E) \geq K_{SKA}(P(ABE))$$

Ueli Maurer *IEEE TIT* 39, 3 (1993)

U. Maurer and S. Wolf, IEEE TIT 45, 2, pp. 499–514, (1999)

Device dependent key – bound by squashed enanglement and relative entropy of entanglement

$(\rho, \mathcal{M})$

Device dependent key K_{DD} is upper bounded by some **entanglement measures**:

$$E_R^\infty(\rho) = \lim_{n\to\infty} \inf_{\sigma\in SEP} \frac{1}{n} D(\rho^{\otimes n}|\sigma) \quad [1]$$

Relative entropy of entanglement

$$K_{DD}(\rho) \leq E_R^\infty(\rho) \quad [2]$$

$$E_{sq}(\rho_{AB}) = \frac{1}{2} \inf_{\Lambda: E\to E'} I(A:B|\mathrm{E}')_{\mathrm{I}_{AB}\otimes\Lambda|\psi_{ABE}\rangle} \quad [3]$$

Squashed entanglement

- Quantum conditional mutual information:

I(AB|E’):=S(AE’)+S(BE’)-S(E’)-S(ABE’)

S(X) – von Neumann entropy of ρ_X

$$K_{DD}(\rho) \leq E_{sq}(\rho) \quad [4]$$

[1] V. Vedral, M. B. Plenio, M. A. Rippin P.L. Knight PRL 78 (12), 2275, (1997)

[2] K., M. P. Horodeccy J. Oppenheim Phys. Rev. Lett **94**, 160502 (2005)

[3] Christandl’s Ms Thesis & M. Christandl A. Winter J. Math. Phys. 45, 3, 829-840 (2004)

[4] Phd thesis of Matthias Christandl (2006)

Non-signaling adversary: bound by squashed non-locality

Complete extension Cext(P)(abe|xyz) of P(ab|xy)

- tripartite conditional probability distribution such that from her share, P(e|z) [1]

Eve can obtain any other non-signaling extension of P(ab|xy)

Squashed non-locality of P(ab|xy) :
intrinsic information computed on action of three parties on the complete extension of P(ab|xy)

$$N_{sq}\big(P(abxy)\big) \coloneqq \max_{xy} \min_{z} I(a:b \downarrow e')\big[\big(M_{xy} \otimes G_z\big) CExt(P(ab|xy))\big]$$ [2]

The key secure against non-signling Eve K_{NSDI} is upper bounded by the squashed non-locality:

$$K_{NSDI}\,(P(ab|xy)) \leq N_{sq}(P(ab|xy))$$

[1] M. Winczewski et al. Quantum 7, 1159 (2023)

[2] M. Winczewski, T. Das, K. H. Phys. Rev. A **106**, 052612 (2022)

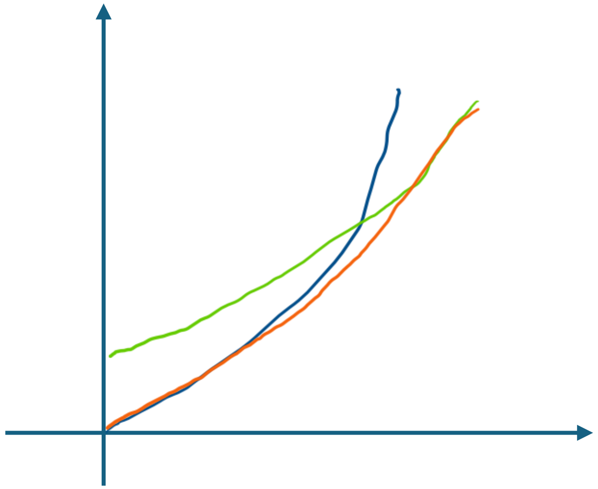
Marek Winczewski’s convexification method

- Squashed non-locality is convex.

⇒the NSDI **key is upper bounded** by a

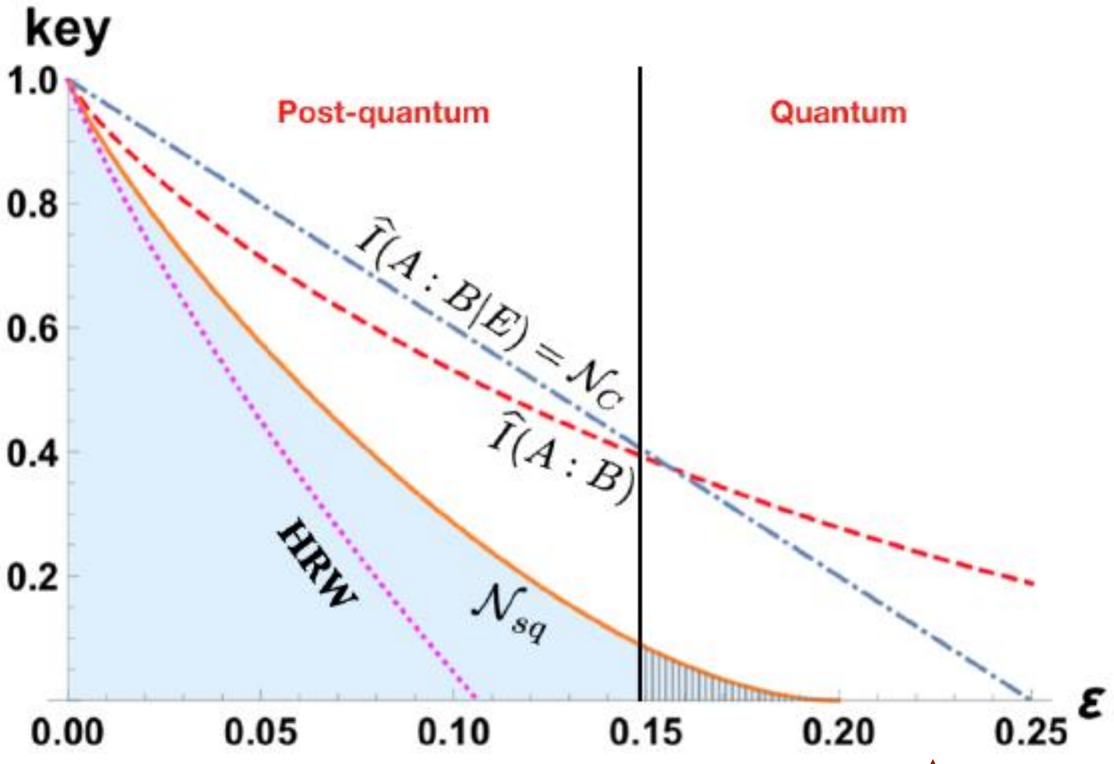
lower convex hull of plots

that upper bound squashed non-locality !



M. Winczewski, T. Das, K. H.
Phys. Rev. A **106**, 052612 (2022)

Non-locality is not sufficient for non-signaling secrecy



Bounds on key for a device

$$P(ab|xy) = (1-\epsilon) \times PR + \epsilon \times \text{antiPR}$$

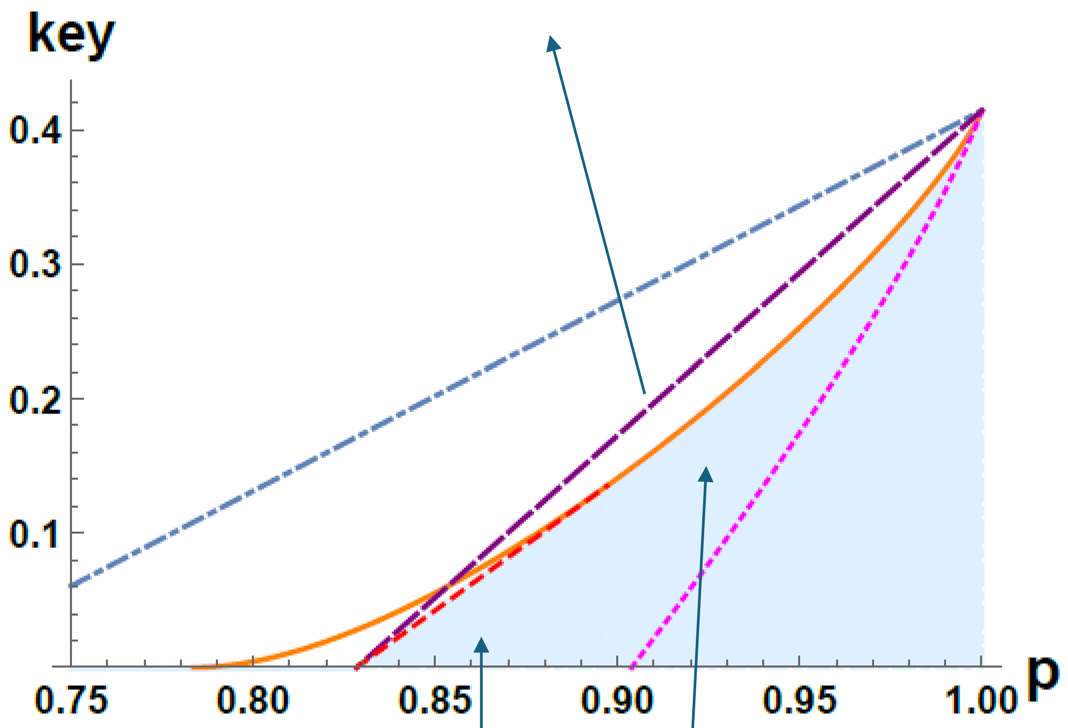
$$PR(ab|xy) = \begin{cases} \frac{1}{2}\ if\ a \oplus b = x.y \\ 0\ else \end{cases}$$

$$antiPR(ab|xy) = \begin{cases} \frac{1}{2}\ if\ a \oplus b = x.y \oplus 1 \\ 0\ else \end{cases}$$

Quantum non-local devices with zero key secret against non-signaling adversary

Results for NSDI QKD
via squashed non-locality + convexification

Bound by Acin Massar and Pironio
New J. Phys., 8:126, 2006.



Tightest numerical bound by convexification method

Our numerical bound

$$
\mathrm{P_{AMP}}(ab|xy) = \begin{array}{cc|cc|cc|cc}
 & x & 0 & & 1 & & 2 & \\
y & b \diagdown a & 0 & 1 & 0 & 1 & 0 & 1 \\
\hline
0 & 0 & \frac{1+p}{4} & \frac{1-p}{4} & \frac{2+\sqrt{2}p}{8} & \frac{2-\sqrt{2}p}{8} & \frac{2+\sqrt{2}p}{8} & \frac{2-\sqrt{2}p}{8} \\
 & 1 & \frac{1-p}{4} & \frac{1+p}{4} & \frac{2-\sqrt{2}p}{8} & \frac{2+\sqrt{2}p}{8} & \frac{2-\sqrt{2}p}{8} & \frac{2+\sqrt{2}p}{8} \\
\hline
1 & 0 & \frac{1}{4} & \frac{1}{4} & \frac{2+\sqrt{2}p}{8} & \frac{2-\sqrt{2}p}{8} & \frac{2-\sqrt{2}p}{8} & \frac{2+\sqrt{2}p}{8} \\
 & 1 & \frac{1}{4} & \frac{1}{4} & \frac{2-\sqrt{2}p}{8} & \frac{2+\sqrt{2}}{8} & \frac{2+\sqrt{2}p}{8} & \frac{2-\sqrt{2}p}{8}
\end{array} .
$$

M. Winczewski, T. Das, K. H.
Phys. Rev. A **106**, 052612 (2022)

(Quantum) device independent key distribution – bound by (quantum)intrinsic non-loclality

?

Non-sig. Quantum E

$$N(\bar{A};\bar{B})_p = \sup_{p(x,y)} \inf_{\rho_{ABXYE}} I(\bar{A};\bar{B}|XYE)_\rho,$$

$\longleftarrow$ *Intrinsic nonlocality*

$\downarrow$

Non-signaling extension

Weaker Eve,
Stronger Alice and Bob

$$K_{NSDIQE}(P(ab|xy)) \leq sup_{P(x,y)} \inf_{Ext(P(ab|xy))} \sum P(x,y)\, I(ab|E)_{Ext(P(ab|xy))}$$

$(\rho, \mathcal{M})?$

$$\rho_{\bar{A}\bar{B}XYE} = \sum_{a,b,x,y} p(x,y)\, \mathrm{Tr}_{AB}[(\Lambda_x^a \otimes \Lambda_y^b \otimes I_E)\rho_{ABE}]\, [a\, b\, x\, y]_{\bar{A}\bar{B}XY},$$

Quantum extension

When extensions come from a single puryfication via local measurement it is Quantum intrinsic non-locality

$$K_{DI}(P(ab|xy)) \leq \; N^Q(\mathsf{A};\mathsf{B})_P := \sup_{P(x,y)} \inf_{\rho_{\mathsf{ABXY}E}} I(\mathsf{A};\mathsf{B}|\mathsf{XY}E)_{\rho_{\mathsf{ABXY}E}}$$

These two measures are faithful i.e.non-zero for all non-local devices

E.Kaur, M. Wilde, A. Winter New. J. of Phys. vol. 22, 0230392020 (2020)

Quantum device independend - bund by reduced entanglement measures

$(\rho, \mathcal{M})?$

$$K_{DI}((\rho, M)) \leq \inf_{(N,\sigma)=(M,\rho)} K_{DD}(\sigma)$$

Corollary: upper bound by **reduced entanglement measures**:

$$K_{DI}(\rho) \leq \min\{\inf_{(N,\sigma)=(M,\rho)} E_{sq}(\sigma), \inf_{(N,\sigma)=(M,\rho)} E_r^{\infty}(\sigma)\}$$

For some states $K_{DI}(\rho) \ll K_{DD}(\rho)$

M. Christandl, R. Ferrara, K. H. Phys. Rev. Lett. **126**, 160501 (2021)

quantum intrinsic information bound

$(\rho, \mathcal{M})?$

- Instead of mimicking the whole P(ab|xy)

Eve can mimick just **Bell inequality violation** S and **quantum bit error rate** Q=$P(a \neq b | x = 0 y = 0)$

For any $S \in [2, 2\sqrt{2}]$ *and* $Q \in [0, 1/2]$,

$$K_{\mathrm{DI}}(S,Q) \leq 1 + h(a_{S,Q}) - h(Q) - h\left((1+\sqrt{(S/2)^2 - 1})/2\right),$$ [1]

where $a_{S,Q} = \frac{1}{2}\left(1 + \sqrt{1 + Q(1-Q)(S^2-8)}\right)$, *and* $h(x) = -x\log x - (1-x)\log(1-x)$ *is the binary entropy.*

$$K_{DI}(S,Q) \leq \inf_{\substack{CHSH(N,\sigma)=S \\ QBER(N,\sigma)=Q}} I(a{:}b \downarrow E)[N_a^{x=0} \otimes N_b^{y=0} \otimes I|\psi_\sigma\rangle]$$ [1], formulation after [2]

(key rounds announced, and key from output)

Quantum Intrinsic Information [3]

[1] R. Arnon -Frideman & F. Leditzky IEEE Trans Inf. Theory 2021

[2] E.Kaur, S.Das, K. H. Phys. Rev. Appl 2021 **18**, 054033 2022

[4] Attack (N, σ) from Pironio et al. New J. of Phys, 11(4):045021, 2009

[3] M. Christandl et al. Proc. 4th Theory of Cryptography Conference, Lecture Notes in Computer Science vol. 4392, pp. 456-478, 2007

$(\rho, \mathcal{M})?$

Convex combination attack

Purely classical strategy of Eve ⇒Intrinsic information bounds the quantum device independent key

- P(ab|xy) = pLocal(ab|xy) + (1-p)NonLocal(ab|xy)

Attack:

- For Local(ab|xy) Eve outputs e = (a,b) [possible whenever Eve **knows the key-generating inputs x=0 y=0**]
- For NonLocal(ab|xy) Eve outputs e = (?)
- Then she optimizes over channels on the output.

Powerful !

$K_{DI}(P(ab|xy)) \leq I(AB \downarrow E)[P(a,b,e|x = 0y = 0)]$ = sometimes zero for non-local devices!

Non-locality is not sufficient resource for standard device independent secure key generation !

M Farkas, Maria Balanzó-Juandó, Karol Łukanowski, Jan Kołodyński, and Antonio Acín Phys. Rev. Lett. 127, 050503 (2021)

Quantum DI bound by cc squashed entanglemenet

$(\rho, \mathcal{M})?$

- Previous bounds:

  Arnon-Frideman&Leditzky uses quantum intrinsic information I(A:B|E) [1]

  - - best in small noise regime
  - **Farkas et al..** uses intrinsic information $I(A:B \downarrow E)$ [2]
  - - best in large noise regime

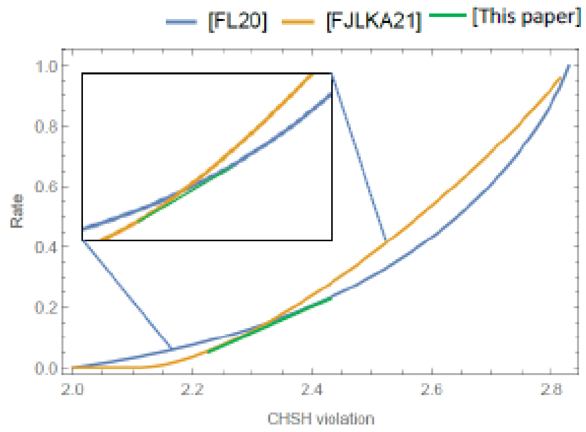
AFL and FBJŁ+ are instances of optimization of **the same functional** given in [1],

Introduced in [3] independently under name cc squashed entanglement

- the cc squashed entanglement is ***convex***

Corollary $\mathrm{K_{DI}}\big(\mathrm{P}(ab|xy)\big) \leq E_{Sq}^{cc}(P) \leq Convex\ hull\ of\,(AFL, FBJŁ+)$ [3]

works well in both noise regimes !



[1] R. Arnon- Friedman and F. Leditzky IEEE Trans. Inf. Theory: 67, 10 (2021)

[2] M Farkas, Maria Balanzó-Juandó, Karol Łukanowski, Jan Kołodyński, and Antonio Acín Phys. Rev. Lett. 127, 050503 (2021)

[3] E.Kaur, S.Das, K. H. Phys. Rev. Appl 2021 **18**, 054033 (2022)

Conference DI quantum secret key – bounds by reduced multipartite squashed entanglement

$(\rho, \mathcal{M})?$

multipartite squashed entanglement [1] + reduction method

+

(multipartie) Quantum Intrinsic Information

=

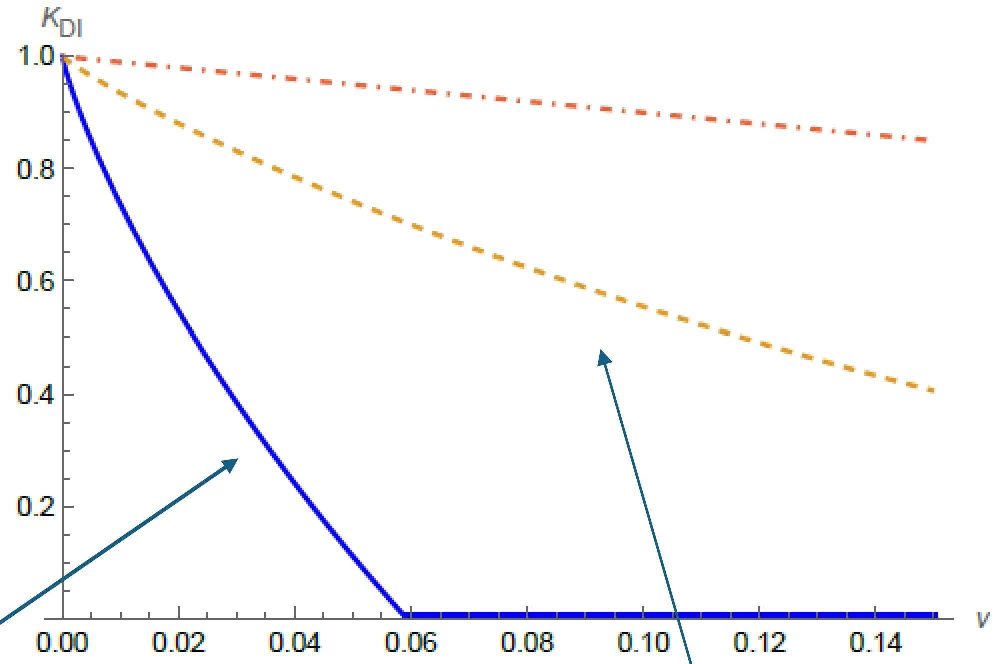
reduced multipartite (cc) squashed entanglement bound [2]

$$I(A_1\colon \ldots \colon A_N|E)_{\sigma_{N(A)}} = \sum_{i=1}^{N} S(A_i|E)_{\sigma_{N(A)}} - S(A_1, \ldots, A_N|E)_{\sigma_{N(A)}}$$

$$K_{DI}\big(\rho_{N(A)}, M\big) \leq \inf_{(\sigma_{N(A)},L)=(\rho_{N(A)},M)} \frac{1}{N-1} I(A_1\colon \ldots \colon A_N \downarrow E)_{L(x)\otimes I\sigma_{N(A)}}$$

[1] Yang et al. IEEE Trans Inf. Theory (2007)
[2] K. H., M. Winczewski, S. Das Phys Rev. A **105**, 022604 (2022)
[see arxiv version and errata to avoid numerous typos ☺)
(for paralel, yet alternative formulation see
[3] A. Philp, E.Kaur, P. Bierhorst M. Wilde Quantum
7 898 (2021)

Multipartie DI QKD – lower and upper bounds $(\rho, \mathcal{M})?$



[Lower bound from
J. Riberio, G. Murta S. Wehner ,
Phys. Rev. A 97, 022307 (2018)

Multipartite cc
squashed
entanglement bound

Key cost and key of formation as upper bounds on device dependent key

$(\rho, \mathcal{M})$

$K_C(\rho)$- how much secure key is needed for creation of a given quantum state by LOCC

$K_F(\rho)$ - minimal average secure key content over ensembles of rho into analogs of pure states in privacy regime

$$K_{DD}(\rho) \ll K_C(\rho) \leq K_F(\rho)$$

K. H., L. Sikorski, S. Das, M. Wilde arXiv:2402.17007

Summary – the family of upper bounds

- Intrinsic information 
- Squashed entanglement $(\rho, \mathcal{M})$
- (quantum) Intrinsic non-locality $(\rho, \mathcal{M})?$? Quantum Eve
- Squashed non-locality ?
- Convex-combination bound and AFL bound $(\rho, \mathcal{M})?$
- (cc-squashed non-locality) $(\rho, \mathcal{M})?$
- Reduced multipartite cc-squashed non-locality $(\rho, \mathcal{M})?$
- Relative entropy of entanglement $(\rho, \mathcal{M})$
- Reduced squashed entanglement & relative entropy of entanglement $(\rho, \mathcal{M})?$
- Loose but operational upper bounds – the key cost & key of formation $(\rho, \mathcal{M})$

Open problems

- Are PPT entangled states useless for DI secure key ?

[conjecture by Rotem Arnon-Friedman and Felix Leditzky]

- Are all entangled states key distillable?
- What is a resource sufficient for DI QKD ?
- Any other new methods of upper bounding secret key ?

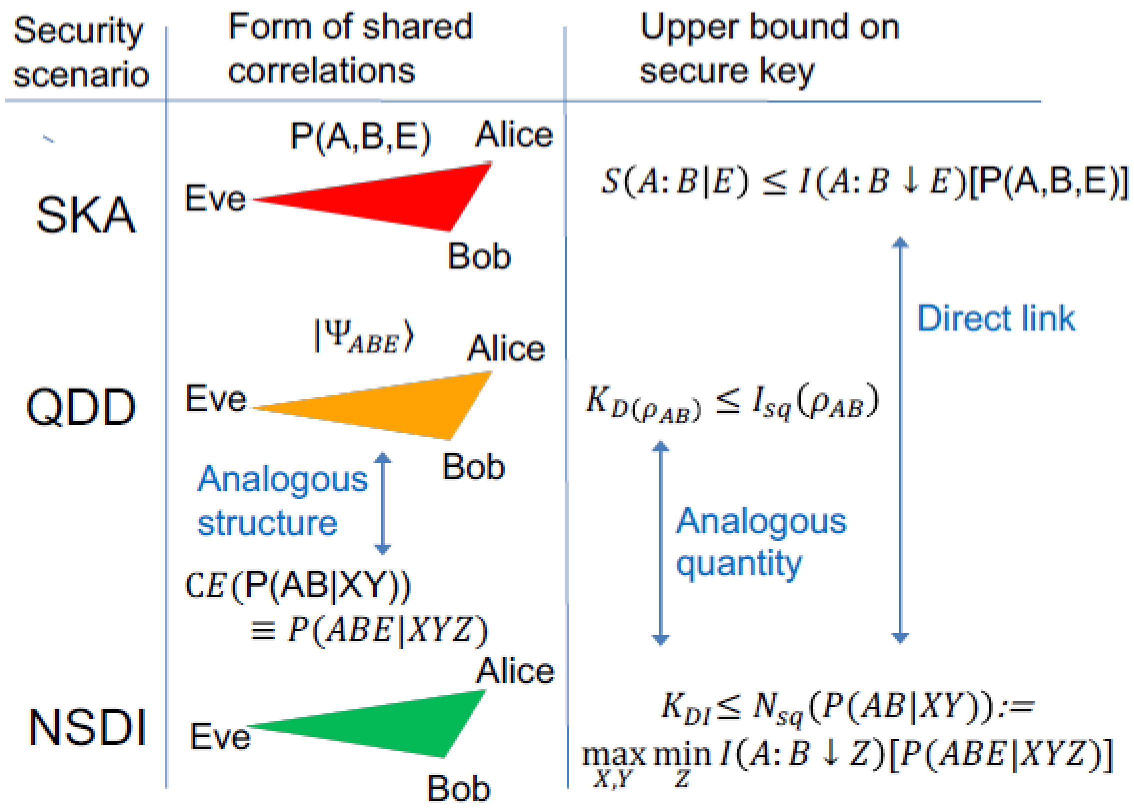
Thank you for your attention ☺

Thank you for your attention ☺

Definition 6 (parity CHSH game [20]). *The parity CHSH inequality extends the CHSH inequality to N parties as follows. Let Alice and Bob$_1$, ..., Bob$_{N-1}$ be the N players of the following game (the parity CHSH game). Alice and Bob$_1$ are asked uniformly random binary questions $x \in \{0,1\}$ and $y \in \{0,1\}$, respectively. The other Bobs are each asked a fixed question, e.g., always equal to 1. Alice will answer bit a, and for all $i \in \{1,\ldots,N-1\}$, Bob$_i$ answers bit b_i. We denote by $\bar{b} \coloneqq \bigotimes_{2\le i\le N-1} b_i$ the parity of all the answers of Bob$_2$, ..., Bob$_{N-1}$. The players win if and only if*

$$a + b_1 = x(y + \bar{b}) \mod 2. \tag{47}$$

Sub-summary



M. Winczewski, T. Das, K. H.
Phys. Rev. A **106**, 052612

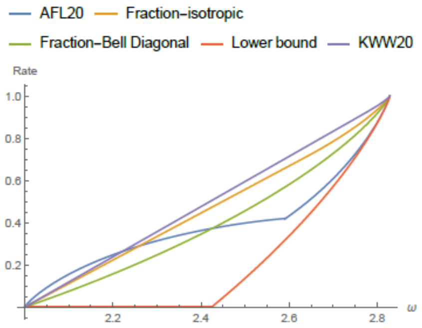
Main result 2: splitting bound

- Previous bound [3]:

$$K_{DI}(P(ab|xy)) \leq \inf_{P(ab|xy)=Tr\, N_x^a \otimes N_y^b \rho} E_R(\sigma)$$

  - $E_R(\rho) = \inf_{\sigma \in SEP} D(\rho||\sigma)$ - relative entropy of entanglement, $P(ab|xy) = (\rho, M)$

$$K_{DI,dev}^{iid}(\rho, M) \leq (1-p) \inf_{(\sigma^{NL},N)=(\rho^{NL},M)} E_R(\sigma^{NL}) + p \inf_{(\sigma^{L},N)=(\rho^{L},M)} E_R(\sigma^{L})$$



  - **Result2**

$$\rho = (1-p)\rho^{NL} + p\rho^{L} \qquad \rho^L, \sigma^L \in LHV, \rho^{NL}, \sigma^{NL} \notin LHV$$

Sometimes zero !

[3] M. Christandl,R. Ferrara, K. Horodecki Phys. Rev. Lett. 126, 160501 (2021)

Gap between DI and DD key

- Matthias Christandl, Roberto Ferrara, Karol Horodecki, *"Upper bounds on device-independent quantum key distribution"* Physical Review Letters **126**, 160501 (2021)

There is a strict gap between Device Independent (DI) and Device Dependent (DD) QKD rates:

There are states for which there does not exist measurements which yield more DI key than DD key

Reduction method, for any upper bound on device dependent key U:

$$K_{DI} \leq \inf_{(\rho,M)=(\sigma,N)} U(\sigma)$$

Main result 3: bounds for elementary channels

- Previous bound [3]

$$K_{DI}(\Lambda, \rho, M) \leq inf_{(\Lambda', \sigma, N)=(\Lambda, \rho, M)} P(\Lambda')$$

  - $(\Lambda, \rho, M) = TrM[\Lambda \otimes I(\rho)]$

  - **Result3** statistics obtained for CHSH protocol for depolarizing channel and erasure

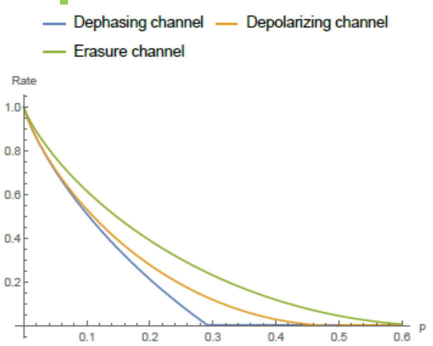
For depolarizing channel, we obtain:

$$\mathcal{P}_i^{IDI_j}(\mathrm{id}_A \otimes \mathcal{D}^p) \leq \min\left\{1 - H\left(\frac{1}{2}(1-\sqrt{1-4p+2p^2})\right), 1 - H(3p/4)\right\}.$$

For erasure channel we obtain:

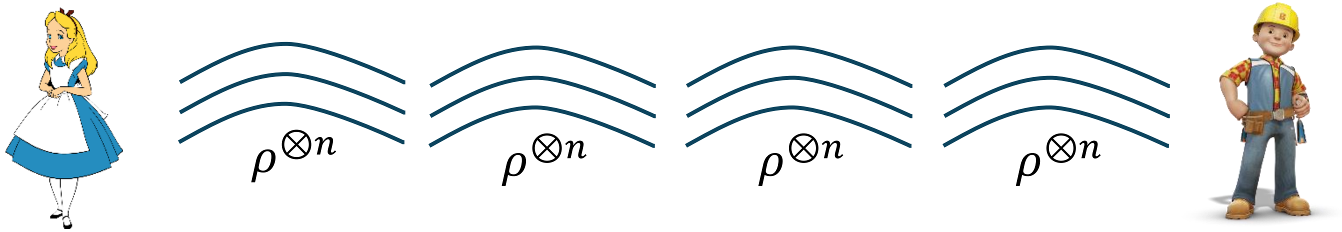
$$\mathcal{P}_i^{IDI_j}(\mathrm{id}_A \otimes \mathcal{E}^p) \leq \min\left\{1 - H\left(\frac{1}{2}(1-\sqrt{1-4p+2p^2})\right), 1 - p\right\}.$$

  - channe … phasing channe



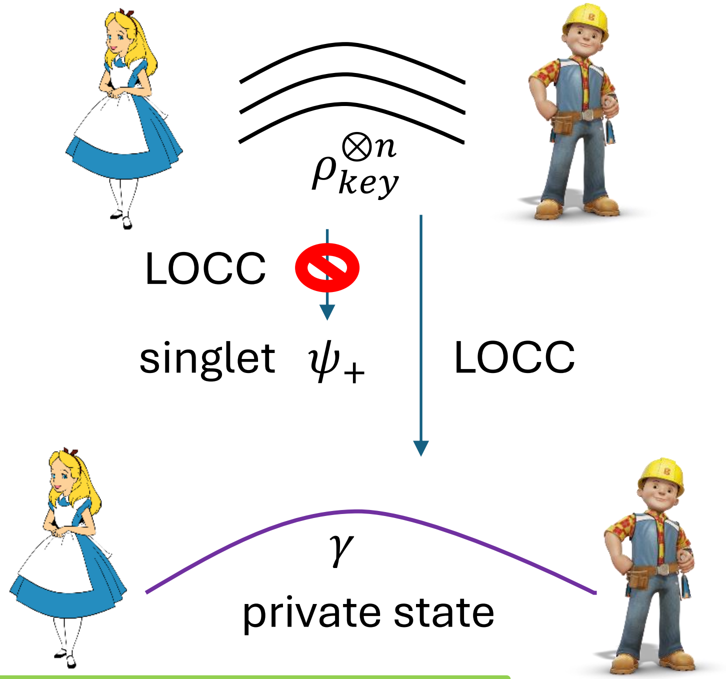
[3] M. Christandl,R. Ferrara, K. Horodecki Phys. Rev. Lett. 126, 160501 (2021)

Key repeaters



Quantum Repeaters $\Leftrightarrow E_D(\rho) > 0$ (possibility of entanglement purification)

- There are states ρ_{key} which have $E_D(\rho_{key}) = 0$, but have $K_D(\rho_{key}) > 0$:



Can we establish quantum KEY repeaters based on distributed ρ_{key} ?

What we know

- Key repeater rate:

$$R_{A\leftrightarrow C\leftrightarrow B}\left(\rho_{AC_A}\otimes\tilde{\rho}_{C_BB}\right) = \inf_{\epsilon>0}\ \limsup_{n\to\infty}\ \sup_{\Lambda_n\in LOCC,\gamma_m}\left\{\frac{m}{n}: Tr_C\Lambda_n\left(\left(\rho_{AC_A}\otimes\ \tilde{\rho}_{C_BB}\right)^{\otimes n}\right)\approx_\epsilon \gamma_m\right\}$$

- Quantum relative entropy :

$$D(\rho||\sigma) = Tr\rho\log\rho - Tr\rho\log\sigma$$

Relative entropy of entanglement:

$$E_R(\rho) = \inf_{\sigma\in\mathrm{SEP}} D(\rho||\sigma)$$

Limitation: $\forall\ \rho\in PPT\ (\ I\otimes T\ \rho\geq 0)$: $R_{A\leftrightarrow C\leftrightarrow B}(\rho\otimes\rho)\leq E_R(I\otimes T\rho)$

[Baeuml, Christandl, Horodecki Winter Nat Com. 2015]

For any private state γ with separable $\hat{\gamma}$: $R^{\rightarrow}(\gamma\otimes\gamma)\leq 2E_D^{\rightarrow}(\gamma)$

[Christandl Ferrara PRL 2016]

Private state after attack

Distillable entanglement with one-way LOCC protocols

Task: Generation of secret key for the one-time pad encription

Secret key – a random bit string of length of the message known only to the honest partis

m – bit string of the message
k - bit string of the key
c - cyphertext

Encoding : $c = k \oplus m$
Decoding : m= $k \oplus c$

One-way key repeater bound for all key corellated states

Karol Horodecki, Leonard Sikorski, Łukasz Pawela, *"Relaxed bound on performance of quantum key repeaters and secure content of generic private and independent bits"*, arXiv:2206.00993

$$\tilde{D}_\alpha(\rho||\sigma) := \frac{1}{\alpha-1}\log_2 \mathrm{Tr}[\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha].$$

Sandwich Renyi relative entropy

$$\tilde{E}_\alpha(\rho) := \inf_{\sigma\in SEP}\tilde{D}_\alpha(\rho||\sigma),$$

(of entanglemet)

$\alpha\to\infty$

$$E_{max}(\rho) = \inf_{\sigma\in SEP}\inf\{\lambda\in \mathrm{R} : \rho\leq 2^\lambda\sigma\}.$$

Max relative entropy of entanglement

A bound for all key correlated states:

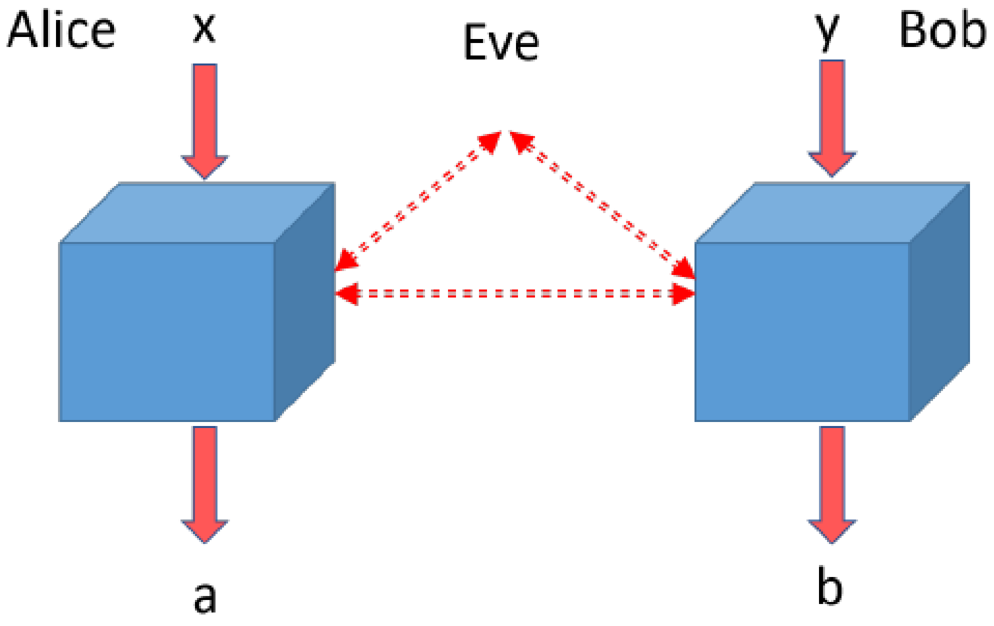
$$\boxed{R^{\rightarrow}(\rho,\rho)\leq 2(\frac{\alpha}{\alpha-1})E_{\vec{D}}(\rho)+2\tilde{E}_\alpha(\hat{\rho}).}$$

where $\phi := \frac{1}{\sqrt{d_k}}\sum_i |i\rangle_A|i\rangle_B$. Then, the *key correlated* state takes form:

$$\rho_{key} := \sum_{\mu,\nu}|\phi_\mu\rangle\langle\phi_\nu|_{AB}\otimes M^{(\mu,\nu)}_{A'B'}, \tag{9}$$

where $M^{(\mu,\nu)}$ are $d_s\times d_s$ matrices on $A'B'$.

Upper bounds on device-independent key



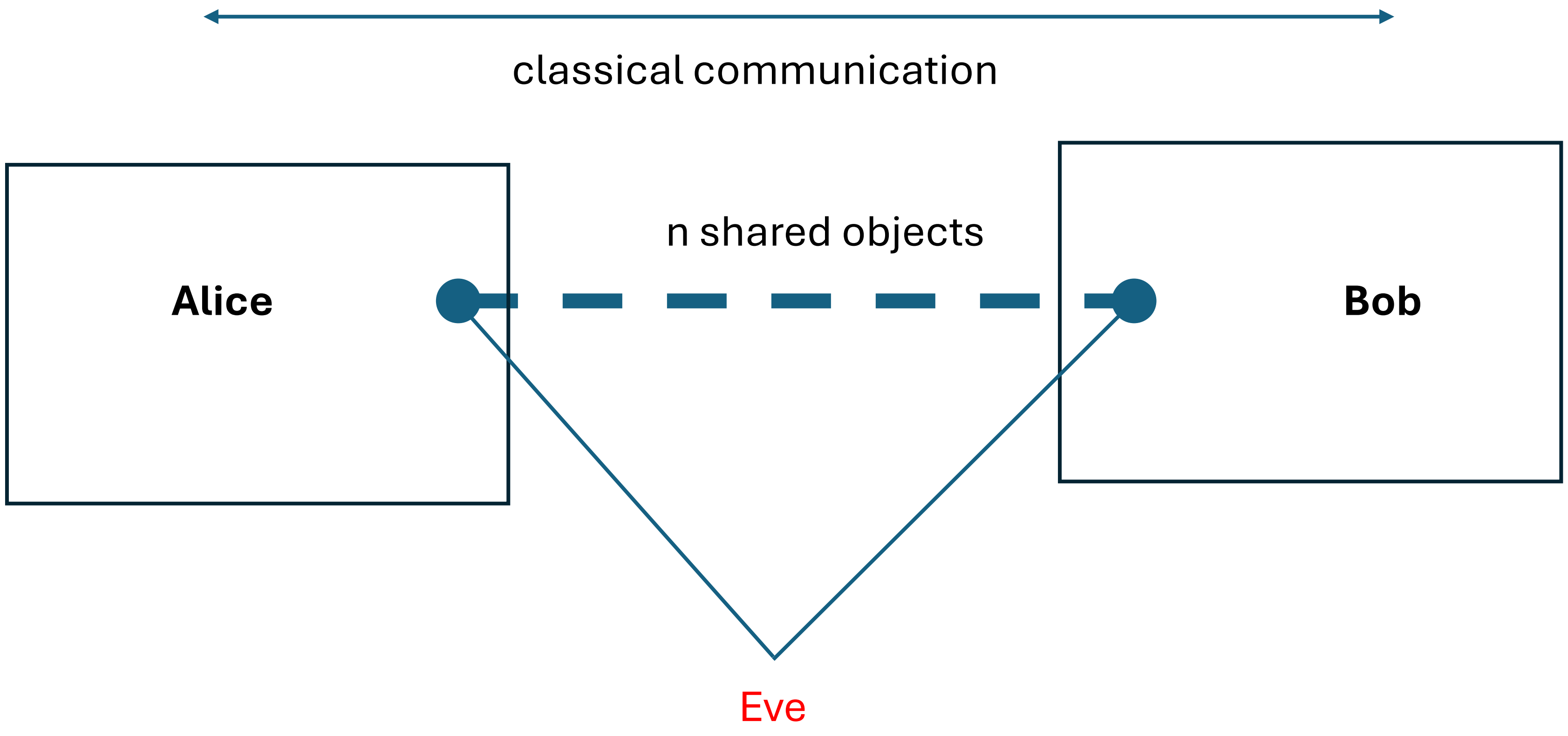
- Scenario of device-independent quantum key distribution
- Main object: P(ab|xy)
- Problem:

$\mathrm{K_{DI}}\big(\mathrm{P}(ab|xy)\big) \leq U(\mathrm{P(ab|xy)})$

for n runs of experiment?

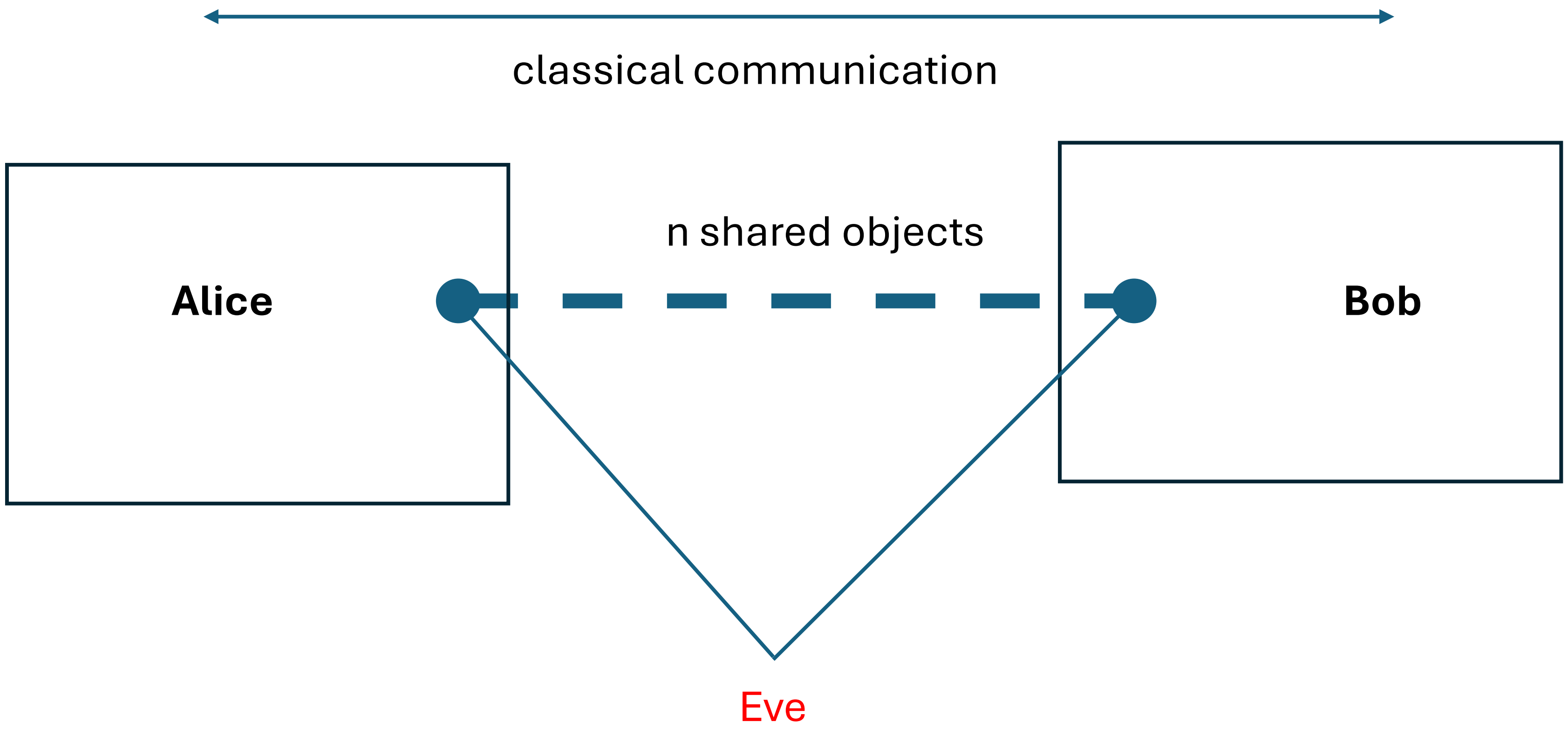
U- some upper bound

Secret key rate



$$\max_{allowed\ operations\ \Lambda}\left\{\frac{k}{n} :\ \Lambda(object_n) \approx secret\ key\ of\ length\ k\right\}$$

Secret key rate



$$\max_{\text{allowed operations } \Lambda} \left\{ \frac{k}{n} : \Lambda(object_n) \approx secret\ key\ of\ length\ k \right\}$$

Current team ☺

Dr Shubhayan Sarkar

Dr Chirag Srivastava

Msc Leonard Sikorski

Msc. Tushita Phrasad

Collaboration with ⟨Z|K⟩

Dr Mikołaj Czechlewski
Dr Paweł Mazurek
Dr Eng. Monika Rosicka
Msc. Maciej Stankiewicz

Dr Eng. Marek Winczewski

University of Gdańsk

National Science Centre Poland

Want to join us in Gdańsk ?

Main two topics : Quantum Energy Initiative
& Quantum cryptography

Phd student position opens in May 2025 (starting in October 2025)
Post-doc position will be open in late 2026.

University of Gdańsk

National Science Centre
Poland