High-dimensional quantum key distribution for multiple measurement bases

Giovanni Chesi[1,2], Nikolai Wyderka[3], Hermann Kampermann[3], Chiara Macchiavello[1,2], Dagmar Bruß[3]

(1) University of Pavia, Physics Department, Pavia
(2) National Institute for Nuclear Physics (INFN), Pavia
(3) Heinrich Heine University, Düsseldorf

Quantum Science Generation
Trento - ETC*, 5-5-2025

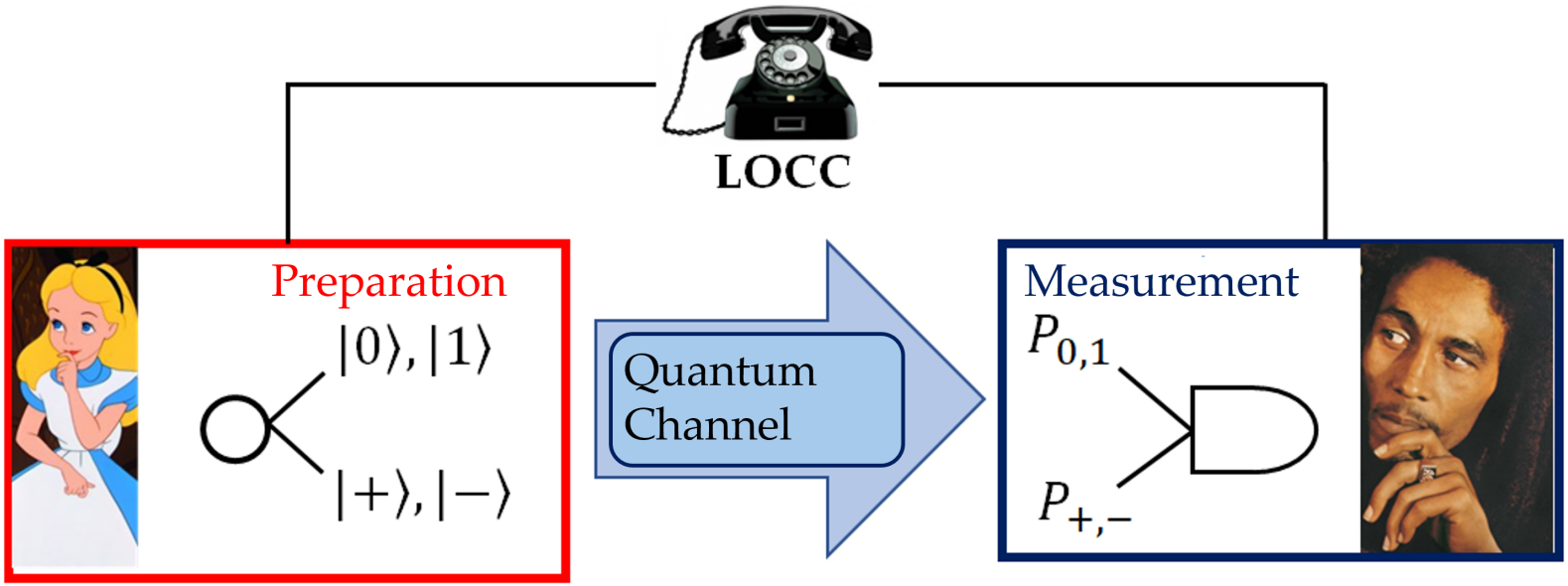
University of Pavia
QUIT quantum information theory group

Outline

- Quantum Key Distribution (QKD)
- The very beginning: the BB84 protocol
- Entanglement-based reformulation: the BBM92 protocol
- From 2D to high-dimensional (HD) states
- Asymptotic key rates
- Finite key rates
  - Proof via the entropic uncertainty relations
  - Proof via the asymptotic equipartition property

Quantum key distribution

The BB84 protocol



Sifting

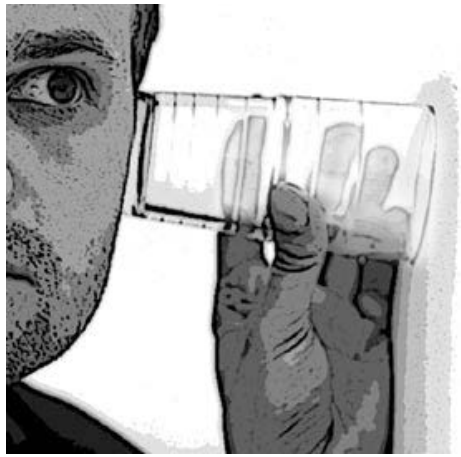
1. σ_z
2. σ_x
3. σ_z
4. σ_x
5. ...

1. σ_z
2. σ_x
3. σ_x
4. σ_z
5. ...

The BB84 protocol

Parameter estimation

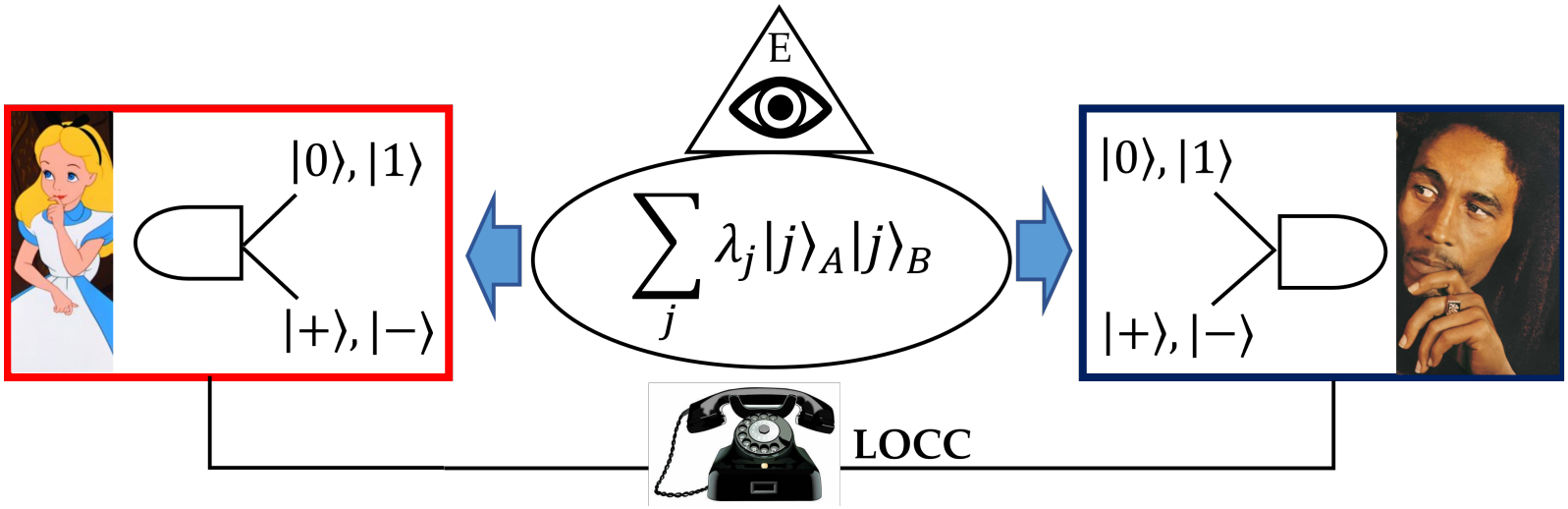
Alice and Bob publicly compare a random subset of their bit lists and compute the *quantum bit error rates* (QBER) for each basis. If the QBERs are larger than a pre-selected threshold, they abort the protocol.



Error correction and privacy amplification

Alice and Bob run an algorithm that match their keys, which are then compressed and secured via hash functions.

The BBM92 protocol



High-dimensional quantum key distribution

From 2D to high dimensional (HD) states

Why?

quBits $\rightarrow$ quDits

HD: information encoded on $d > 2$ orthogonal states. Advantages:

- higher secret key rates
- higher maximum tolerable error rate
  maximum tolerable = maximum error rate s.t. the key rate is non-zero

D. Bruss and C. Macchiavello, *Phys. Rev. Lett.* **88** (2002)

N.J. Cerf, M. Bourennane, A. Karlsson and N. Gisin, *Phys. Rev. Lett.* **88** (2002)

- a larger number m of *mutually unbiased bases* can be exploited

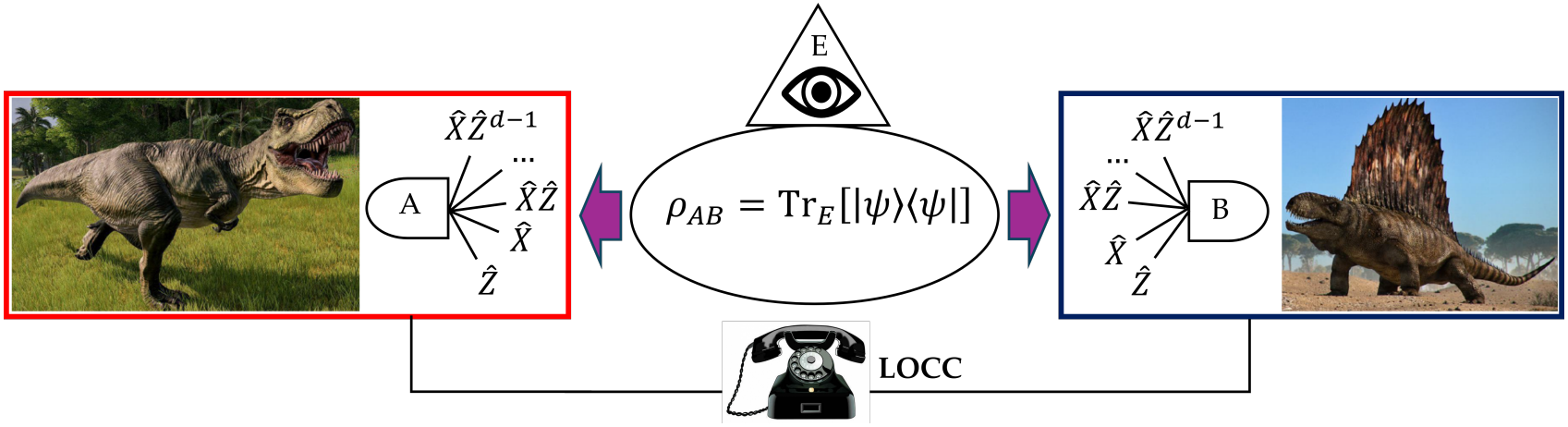
S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury and F. Vatan, *Algorithmica* **34** (2002)

- experimentally feasible (e.g. TMs of single photon states)

B. Brecht, D. V. Reddy, C. Silberhorn and M. G. Raymer, *Phys. Rev. X* **34** (2002)

From 2D to high dimensional (HD) states

HD BBM92

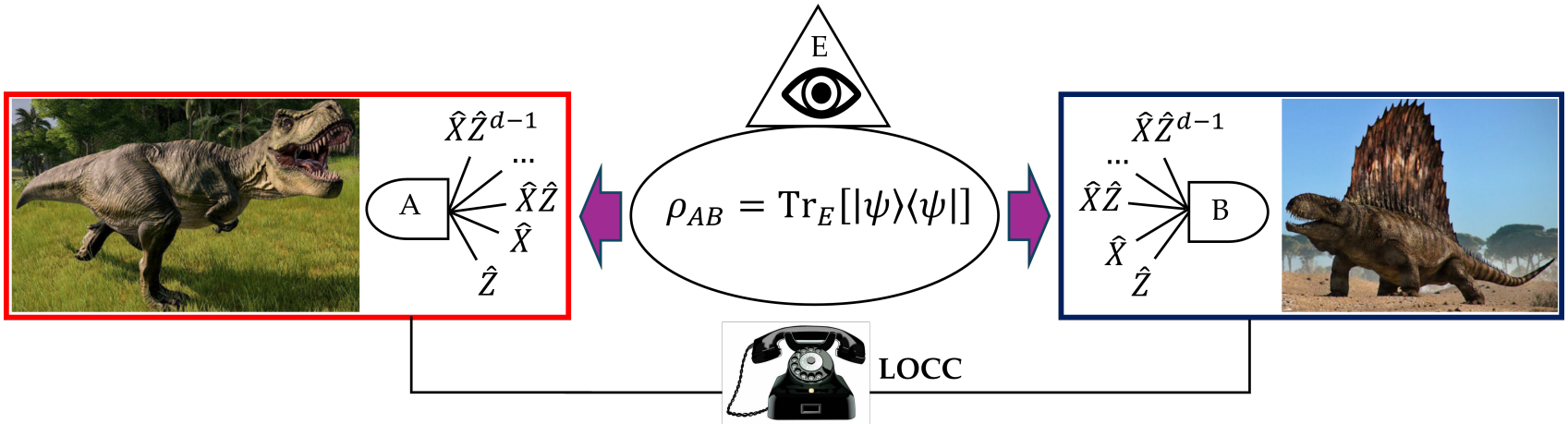


Preparation

- $|\psi\rangle \in \mathscr{H}_{ABE}$
- HD Bell states: $|\phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle$, $|\phi_{\alpha,\beta}\rangle = \mathbb{1} \otimes X^\alpha Z^\beta |\phi^+\rangle$
- with $X \equiv \sum |j\rangle\langle j-1|$, $Z = \sum e^{2\pi i j/d} |j\rangle\langle j|$
- $\tilde{\rho}_{AB} = \sum_{\alpha,\beta=0}^{d-1} \lambda_{\alpha,\beta} |\phi_{\alpha,\beta}\rangle\langle\phi_{\alpha,\beta}|$ (Bell-diagonal state)

From 2D to high dimensional (HD) states

HD BBM92

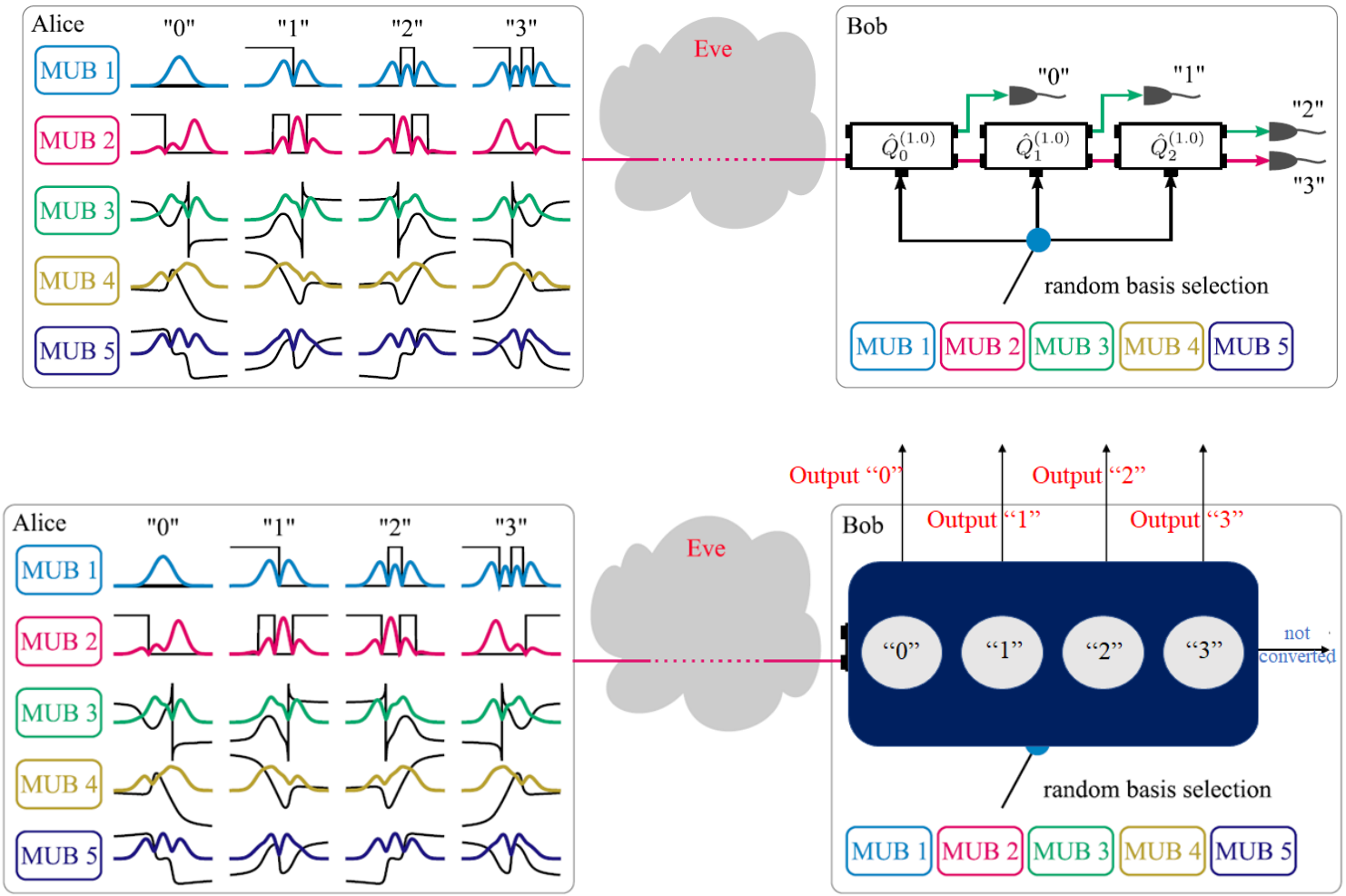


Measurement

- set of m mutually unbiased bases (MUBs) $Z, X, XZ..., XZ^{m-2}$
- if d is a prime power, there are up to $d+1$ MUBs; if d is not, just sets of *three* MUBs are known
- *error rates*:
  $Q_Z = 1 - \sum_{\alpha=0}^{d-1} \lambda_{0,\alpha}$, $Q_{XZ^k} = 1 - \sum_{\alpha=0}^{d-1} \lambda_{\alpha,k\alpha}$

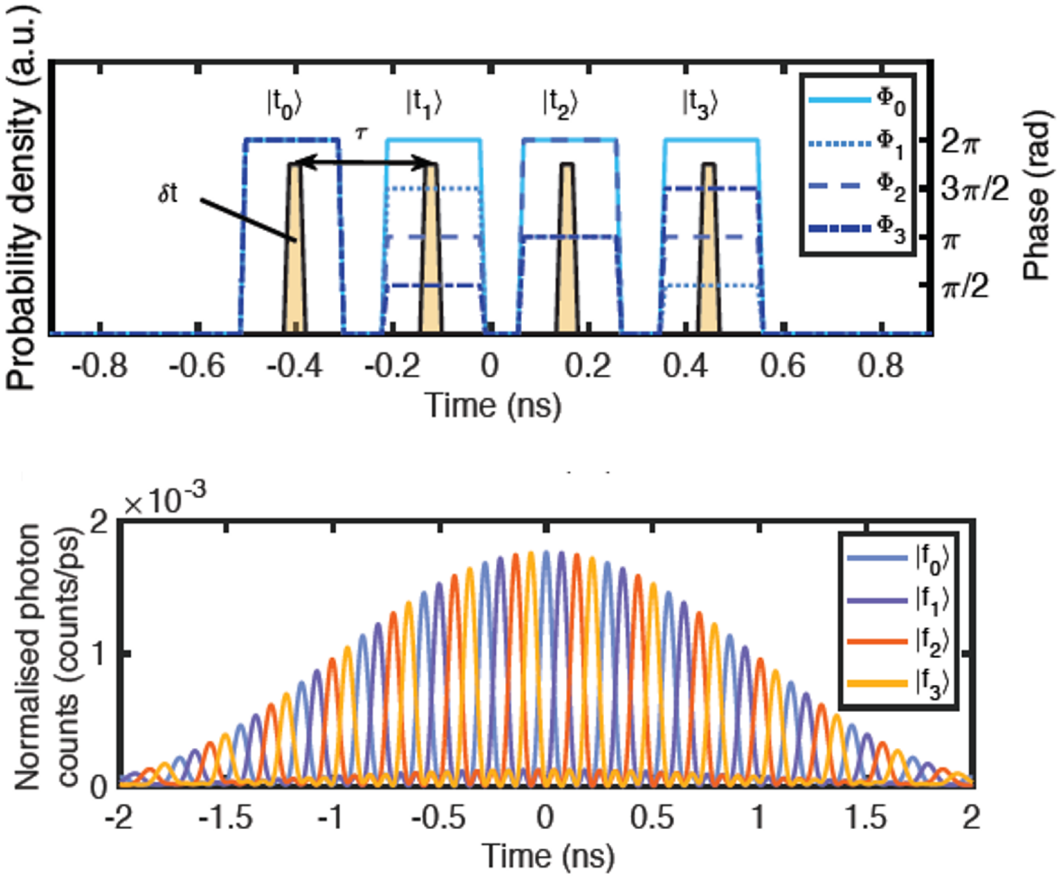
Experimental implementations

Temporal modes



B. Brecht, D. V. Reddy, C. Silberhorn and M. G. Raymer, *Phys. Rev. X* **34** (2002)

Experimental implementations



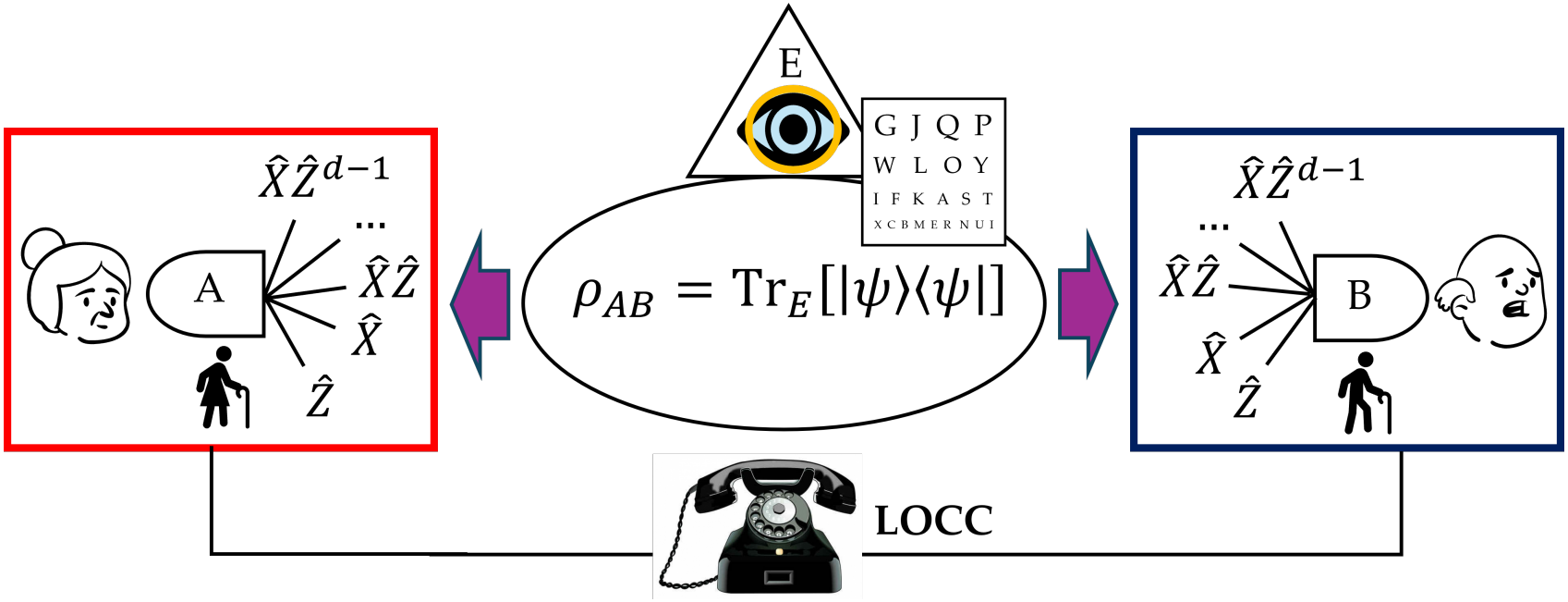
M. Ogrodnik, A. Widomski, D. Bruß, G. Chesi, F. Grasselli, H. Kampermann, C. Macchiavello, N. Walk, N. Wyderka and M. Karpiński, arXiv:2412.16782 [quant-ph] (2025)

Results

N. Wyderka, G. Chesi, H. Kampermann, C. Macchiavello and D. Bruß, arXiv:2501.05890 [quant-ph] (2025)

Asymptotic regime

In the limit of an infinite number of rounds $N \to \infty$,



Devetak-Winter rate [I. Devetak and A. Winter, *Proc. R. Soc. A.* **461** (2005)]

$$r_\infty \equiv I(R_A : R_B) - I(R_A : E)$$

with $I(X:Y) = H(X) + H(Y) - H(X,Y)$, the *mutual information*
R_A, R_B raw keys of Alice and Bob.

Asymptotic regime

$$\mathrm{I}(R_A:R_B)-\mathrm{I}(R_A:E)\leq H(R_B)-H(E)=\log_2(d)-H(A,B)_{\tilde{\rho}_{AB}}$$

Maximization of Eve's information

$$\min_{\tilde{\rho}_{AB}} \quad \log_2(d)-H(A,B)_{\tilde{\rho}_{AB}}$$

$$\text{subject to } \; Q_j \text{ as observed, } j\in\{Z,X,XZ,\ldots\}.$$

Case $m=d+1$

$$\mathrm{r}_\infty^{(m=d+1)}=\log_2 d\overbrace{+q\log_2 q+(1-q)\log_2(1-q)}^{-h(q)}-q\log_2(d^2-1)$$

where here $Q_X=Q_Z=Q_{XZ^k}=Q\ \forall k$ and $q=(d+1)Q/d$.

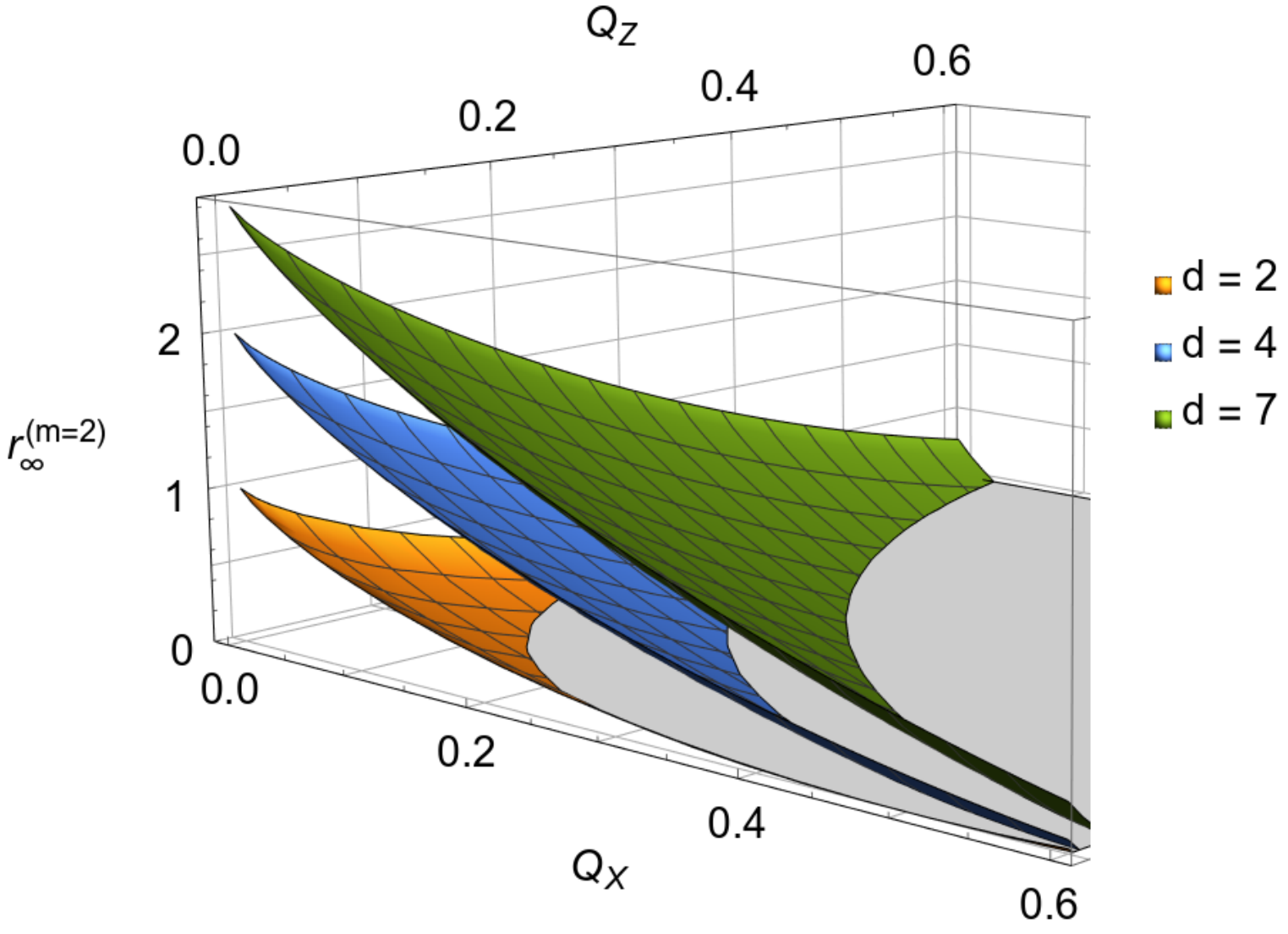
Case $m<d+1$

No analytic result, except for $m=2$:

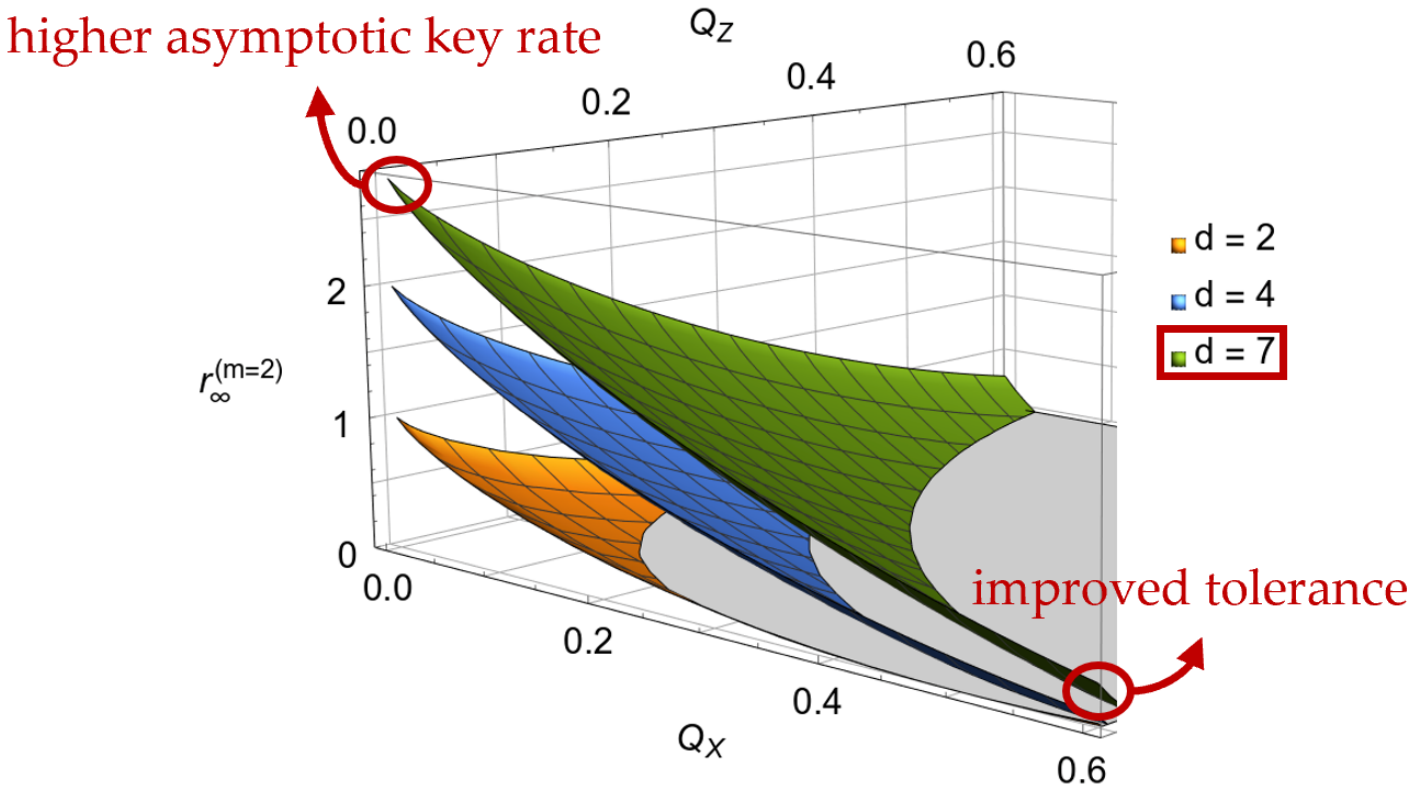
$$\mathrm{r}_\infty^{(m=2)}=\log_2 d-h(Q_X)-h(Q_Z)-(Q_X+Q_Z)\log_2(d-1).$$

Asymptotic key rate

$m = 2$, asymmetric error rates

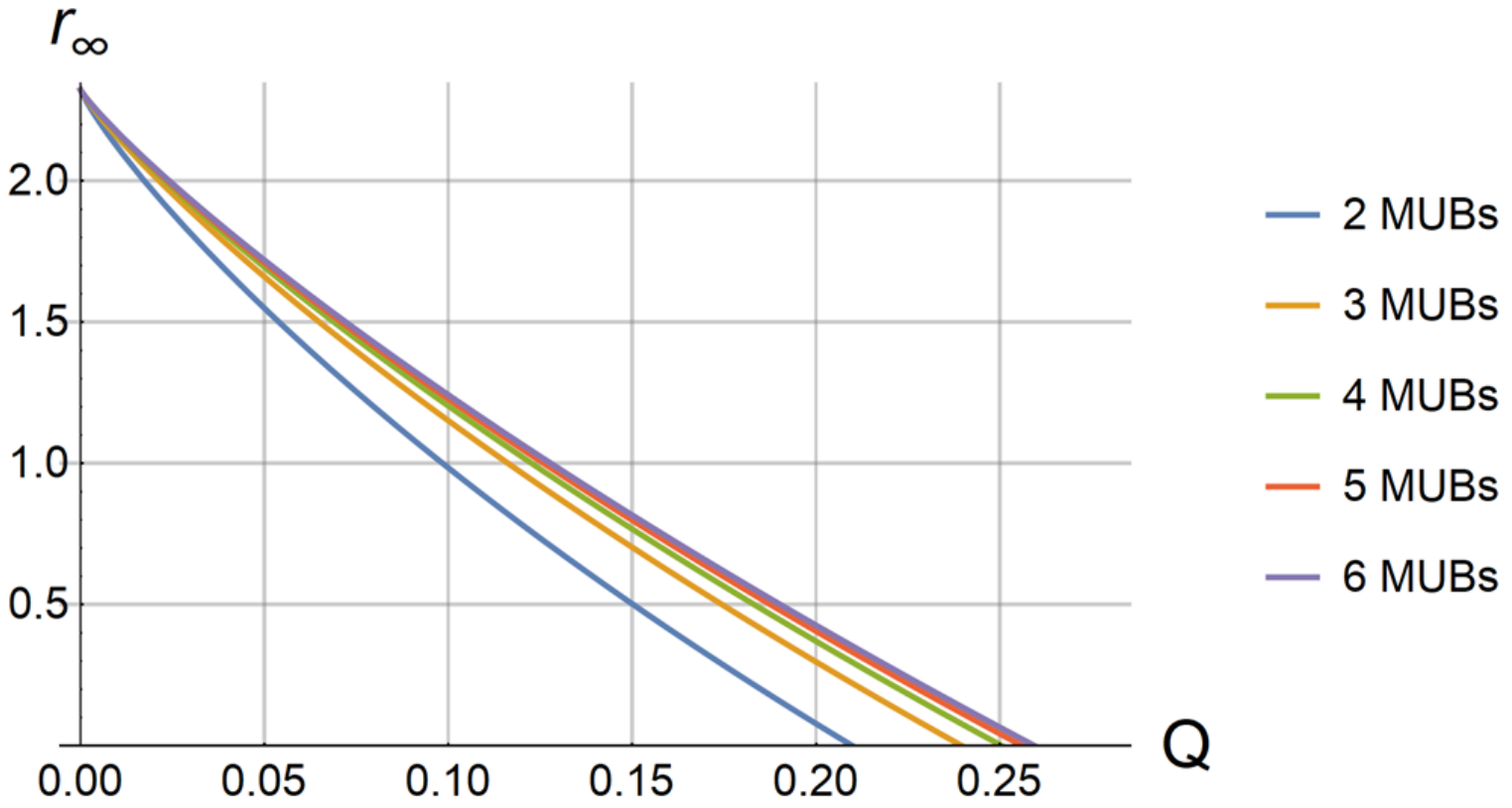


Asymptotic key rate
$m = 2$, asymmetric error rates



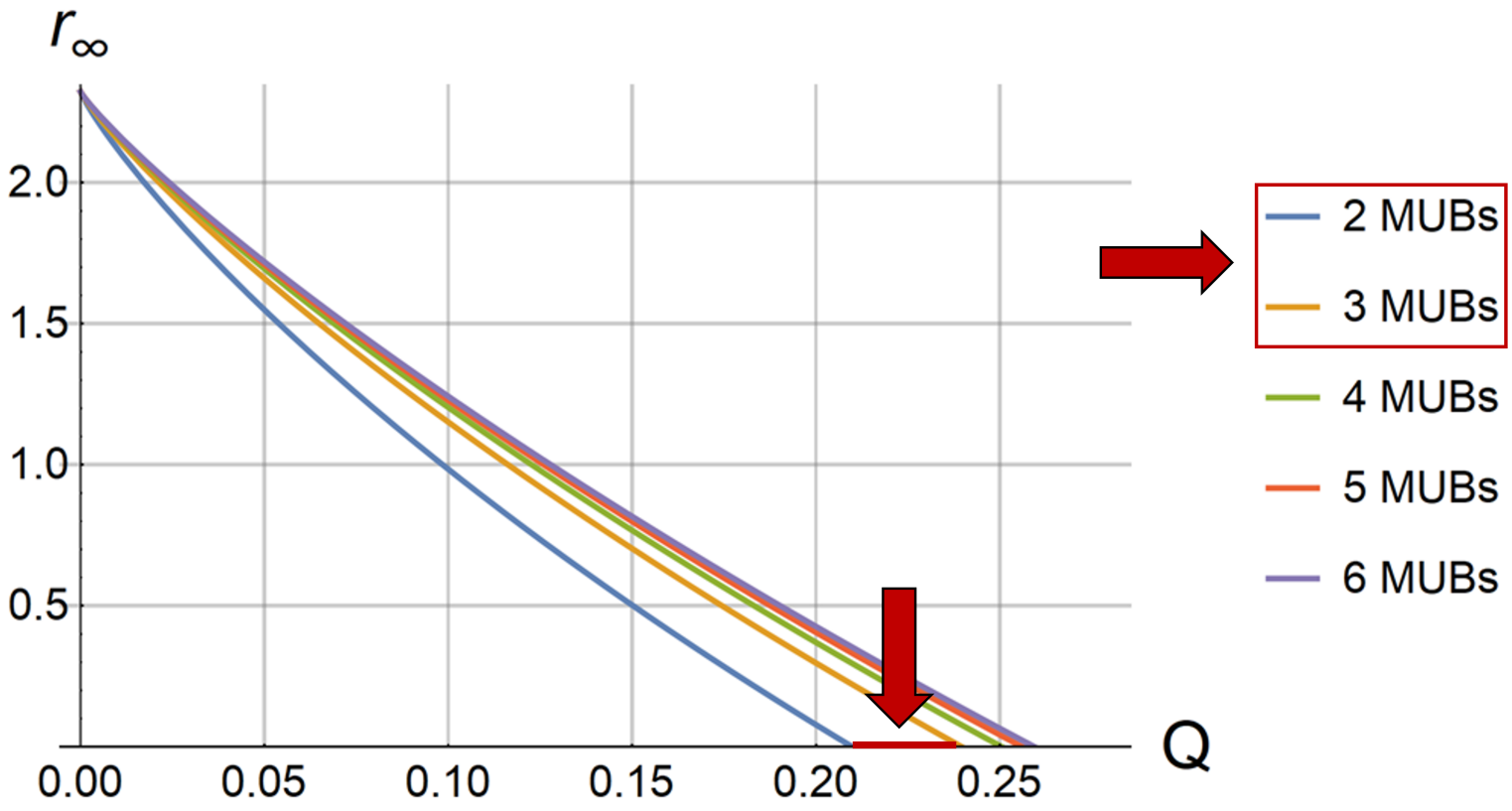
Asymptotic key rate

$d = 5$, symmetric error rates



Asymptotic key rate

$d = 5$, symmetric error rates



Compare with K. Brádler, M. Mirhosseini, R. Fickler, A. Broadbent and R. Boyd, *New J. Phys.* **18** (2016).

Finite regime

After *error correction* (EC) and *privacy amplification* (PA), the length of the key is reduced to

$$l \leq H_{\min}^{\varepsilon}(Z_A^n|E) - \text{leak}_{\text{EC}} - \log_2 \frac{2}{\varepsilon_{\text{EC}}} - 2\log_2 \frac{1}{2\varepsilon_{\text{PA}}}$$

which is ε_{tot}-secure with $\varepsilon_{\text{tot}} = \varepsilon + \varepsilon_{\text{PA}} + \varepsilon_{\text{EC}}$.

- Z: *key generation basis*, n rounds
- $X, XZ..., XZ^{m-2}$: *test bases*, k rounds
- $n + k = N$.

M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, *Nat. Comm.* **3**, 634 (2012)

R. Renner and R. König, *Theory of Cryptography* 3378, Springer (2005)

Bounding $H_{\min}^{\varepsilon}(Z_A^n|E)$

- entropic uncertainty relation
- asymptotic equipartition property

Proof via the entropic uncertainty relation

Uncertainty relation for smooth entropies

$$H_{\min}^{\varepsilon}(Z_A^n|E) \geq nC - H_{\max}^{\varepsilon}(X_A^k|X_B^k)$$

M. Tomamichel and R. Renner, *PRL* **106**, 110506 (2011)

- $C \equiv$ compatibility factor (for projective measurements, $C = \log_2 d$)
- $Q_{\text{tol}} \equiv$ maximum error tolerance
- $\mu_\varepsilon \equiv$ statistical uncertainty

$$H_{\max}^{\varepsilon}(X_A^k|X_B^k) \leq n[h(Q_{\text{tol}} + \mu_\varepsilon) + (Q_{\text{tol}} + \mu_\varepsilon)\log_2(d-1)]$$

M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, *Nat. Comm.* **3**, 634 (2012).

$$\mathrm{r}(\varepsilon, \varepsilon_{\text{EC}}, \varepsilon_{\text{PA}}, n, k) \leq C - h(Q_{\text{tol}} + \mu_\varepsilon) - (Q_{\text{tol}} + \mu_\varepsilon)$$
$$\cdot \log_2(d-1) - \frac{1}{n}\left(\text{leak}_{\text{EC}} + \log_2 \frac{2}{\varepsilon_{\text{EC}}} + 2\log_2 \frac{1}{2\varepsilon_{\text{PA}}}\right)$$

Proof via the asymptotic equipartition property

Asymptotic equipartition property

For $n \geq 8(1-2\log_2 \varepsilon)/5$,

$$\frac{1}{n} H_{\min}^{\varepsilon}(Z_A^n|E) \geq H(Z_A|E)_{\tilde{\rho}_{AB}} - \frac{4}{\sqrt{n}} \log_2(2+\sqrt{d}) \sqrt{\log_2 \frac{2}{\varepsilon^2}}$$

M. Tomamichel, R. Colbeck, and R. Renner, *IEEE Trans. Inf. Theory* **55**, 5840 (2009).

$$\mathrm{r}(\varepsilon_{\mathrm{tot}}, N, n, m, Q) = \frac{n}{N} \underbrace{[\min_{\tilde{\rho}_{AB}} (H(Z_A|E) - \mathrm{leak}_{\mathrm{EC}})]}_{r_{\infty}^{(m)}(Q_{\mathrm{tol}}+\mu_{\varepsilon})}$$

$$- \frac{1}{N} \left[\log_2 \frac{1}{2\varepsilon_{\mathrm{EC}} \varepsilon_{\mathrm{PA}}^2} + 4\sqrt{n} \log_2(2+\sqrt{d}) \sqrt{\log_2 \frac{2}{\varepsilon^2}} \right]$$

Comparison

Uncertainty relation

- secure against *coherent attacks*
- holds for $m = 2$ bases
- an extension for $m > 2$ has been suggested, but have some issues still to be solved

  R. Wang et al., *Phys. Rev. Res.* **3**, 023019 (2021).

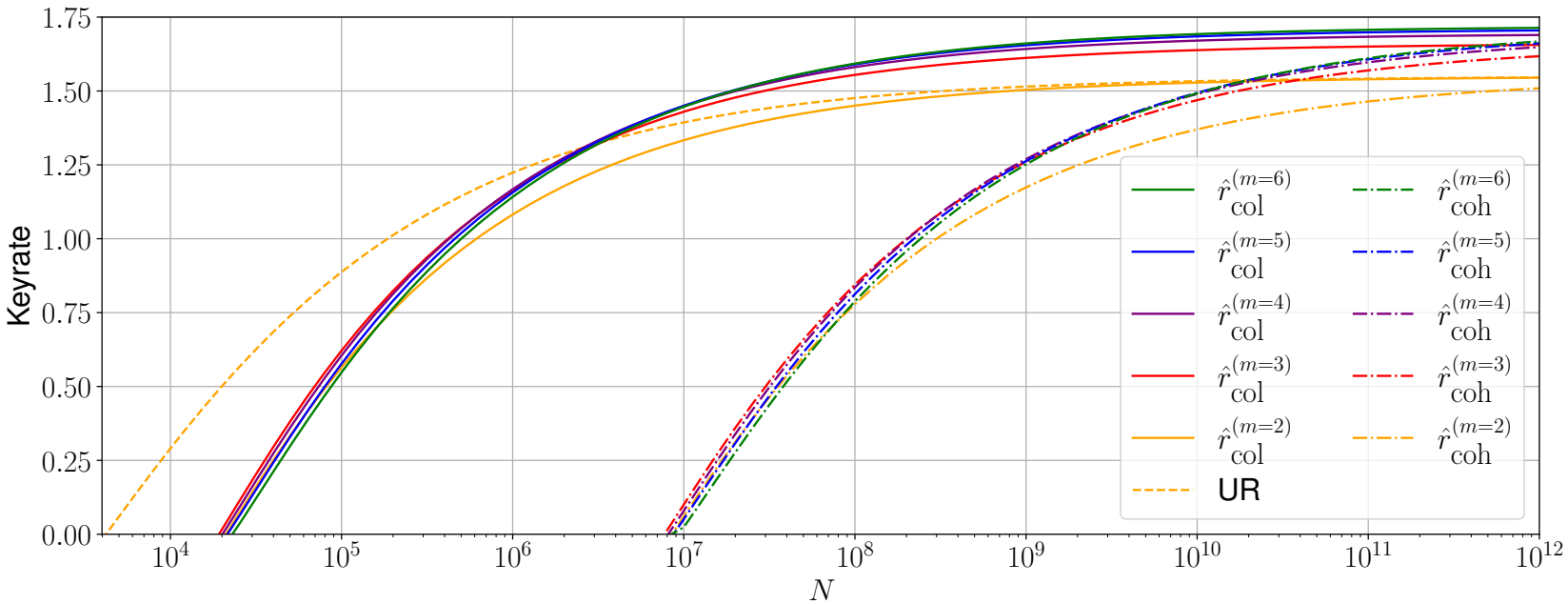
Asymptotic equipartition property

- holds for every allowed number of bases
- secure against *collective attacks*
- security can be generalized to coherent attacks through the *post-selection technique (PST)*
- but the PST has been found to yield too optimistic rates

  S. Nahar et al., *PRX Quantum* **5**, 040315 (2024).

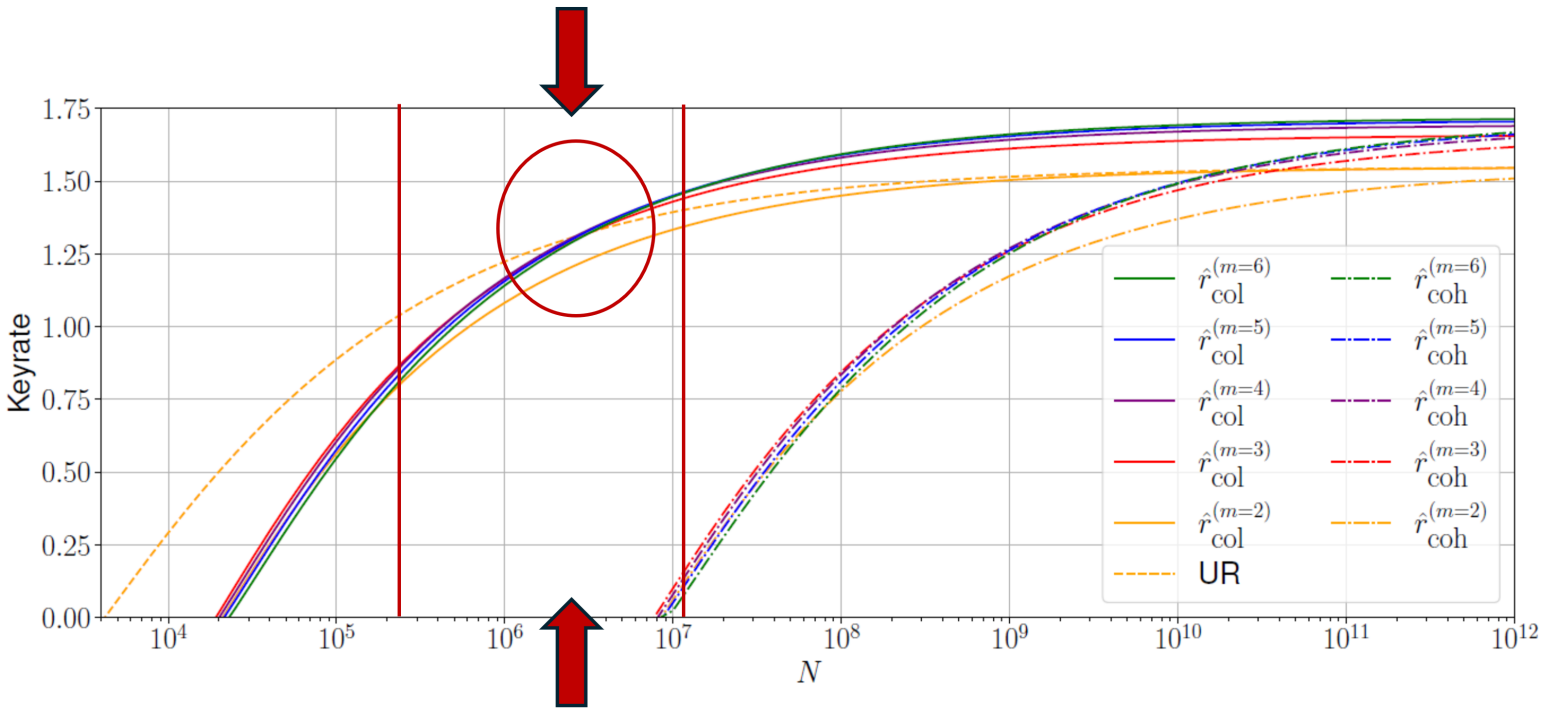
Finite key rate

$d = 5$



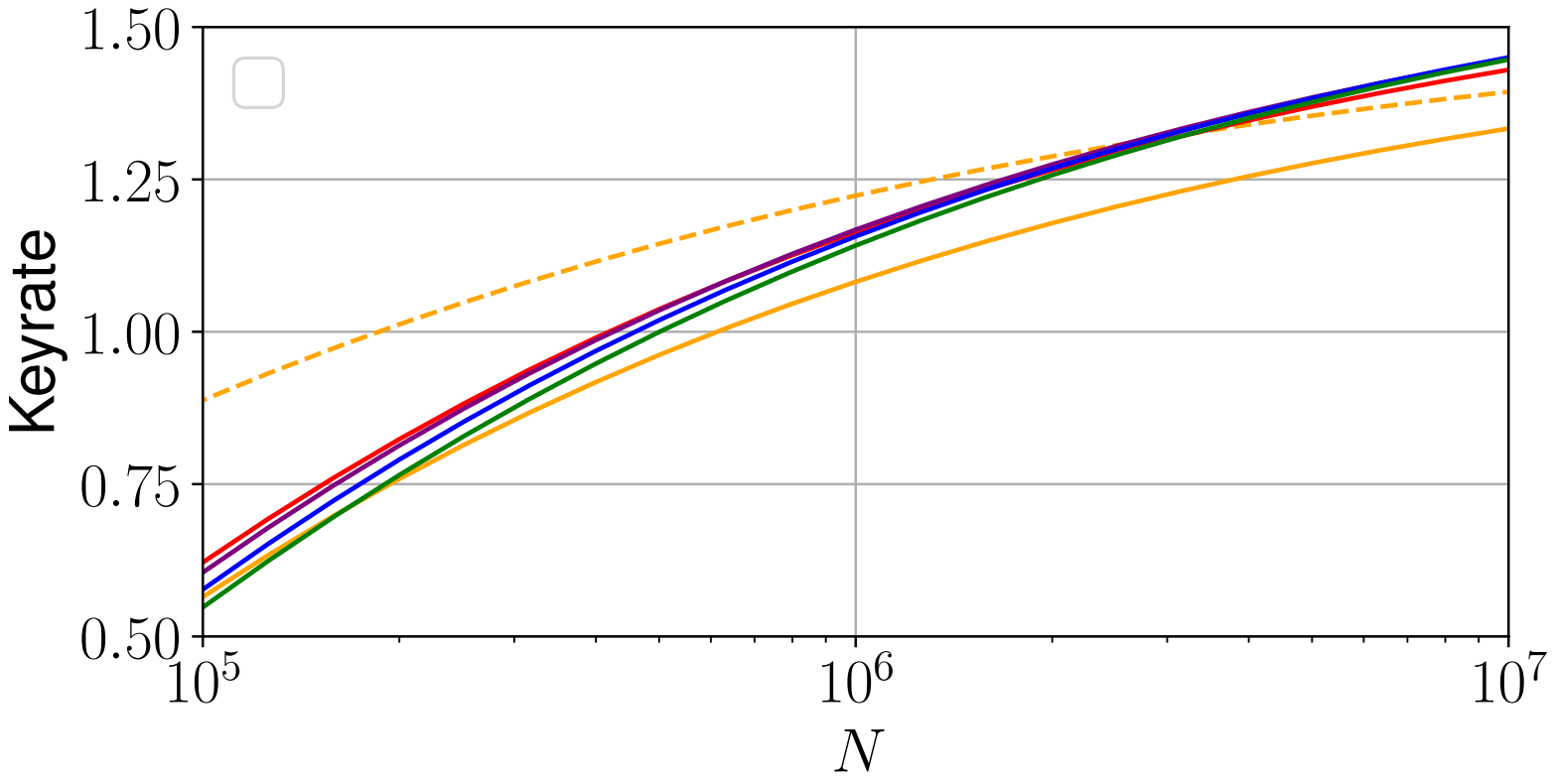
Finite key rate

$d = 5$



Finite key rate

$d = 5$



Conclusions

- HD encodings can be used to enhance the security and the efficiency of QKD protocols with
  - improved secret key rates
  - improved tolerance to errors
- for an asymptotically large number of rounds,
  - the maximum tolerable error rate increases as the number of MUBs employed increases
  - but as m increases the relative improvement shrinks: by selecting $m = 3$, one gets nearly optimal tolerance
- in the finite regime, the results obtained through the asymptotic equipartition property shows a threshold $\bar{N}$ on the number of rounds such that for $N < \bar{N}$ the optimal key rate is obtained with $m = 3$ MUBs.

Thank you!