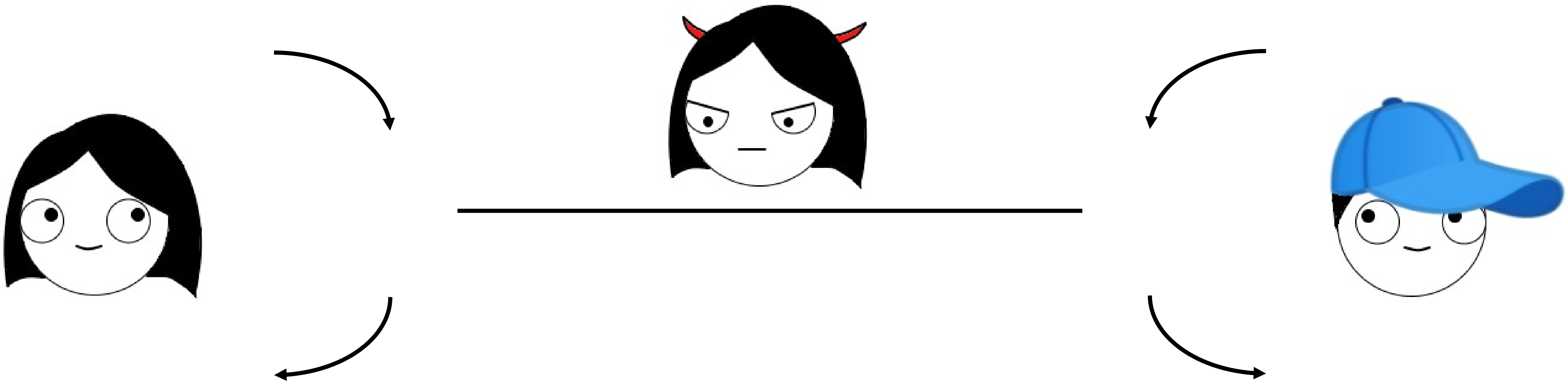
Finite-size DIQKD with noisy preprocessing and random key measurements

Ernest Y.-Z. Tan, Pavel Sekatski, Jean-Daniel Bancal, Xavier Valcarce, René Schwonnek, Renato Renner, Nicolas Sangouard, Charles C.-W. Lim

[SBV+20] arXiv:2009.01784
[TSB+20] arXiv:2012.08714

Device-independent scenario



Bell violation ⇒ is entangled

Regardless of measurements or system dimension!

Prospects for DIQKD

Benefits:

- New level of security
- Improved resistance to hacking

Challenges:

- Security analysis is difficult
- Low noise tolerance

Recent proposals for improvement → Low noise tolerance

Protocol variant: Noisy preprocessing

Key-generating measurements

One-way keyrate:

Alice adds (trusted) noise

[HST+20] arXiv:2005.13015

Protocol variant: Random key measurements

Key-generating measurements

One-way keyrate:

[SGP+20] arXiv:2005.02691

Previous results: key features

- Based on CHSH inequality

Go beyond CHSH?

- DIQKD possible asymptotically
  - Noisy preprocessing: Photons
  - Random key measurements: NV centres, cold atoms

Finite-size analysis?

Combine variants?

- (Recent important developments, will return later)

Our contributions

- "Device-independent quantum key distribution from generalized CHSH inequalities", [SBV+20] arXiv:2009.01784
  - Beyond CHSH (+ noisy preprocessing)
  - Preceded by [WAP20] arXiv:2007.16146

- "Improved DIQKD protocols with finite-size analysis", [TSB+20] arXiv:2012.08714
  - Combines protocol variants
  - Algorithm to compute keyrates ($\rightarrow$ new noise tolerance thresholds)
  - Finite-size analysis

Overview

- Part 1: Asymptotic keyrates
  - [SBV+20] Beyond CHSH (+ noisy preprocessing)
  - [TSB+20] Combining all variants
  - New depolarizing-noise threshold
- Part 2: Finite-size analysis
  - Several technical improvements
  - Consider existing Bell tests
- Outlook and recent developments

Part 1: Asymptotic keyrates

- Typically in (DI)QKD protocol:
  - Perform parameter estimation
  - Abort if observed values outside "acceptable" range
- Main security proof requirement:

Asymptotic keyrate

Lower-bound minimum

over "acceptable" states and measurements

Focus on 2-input 2-output: use "qubit reduction"

Tilted CHSH inequalities [SBV+20]

- Security based on value of

CHSH:

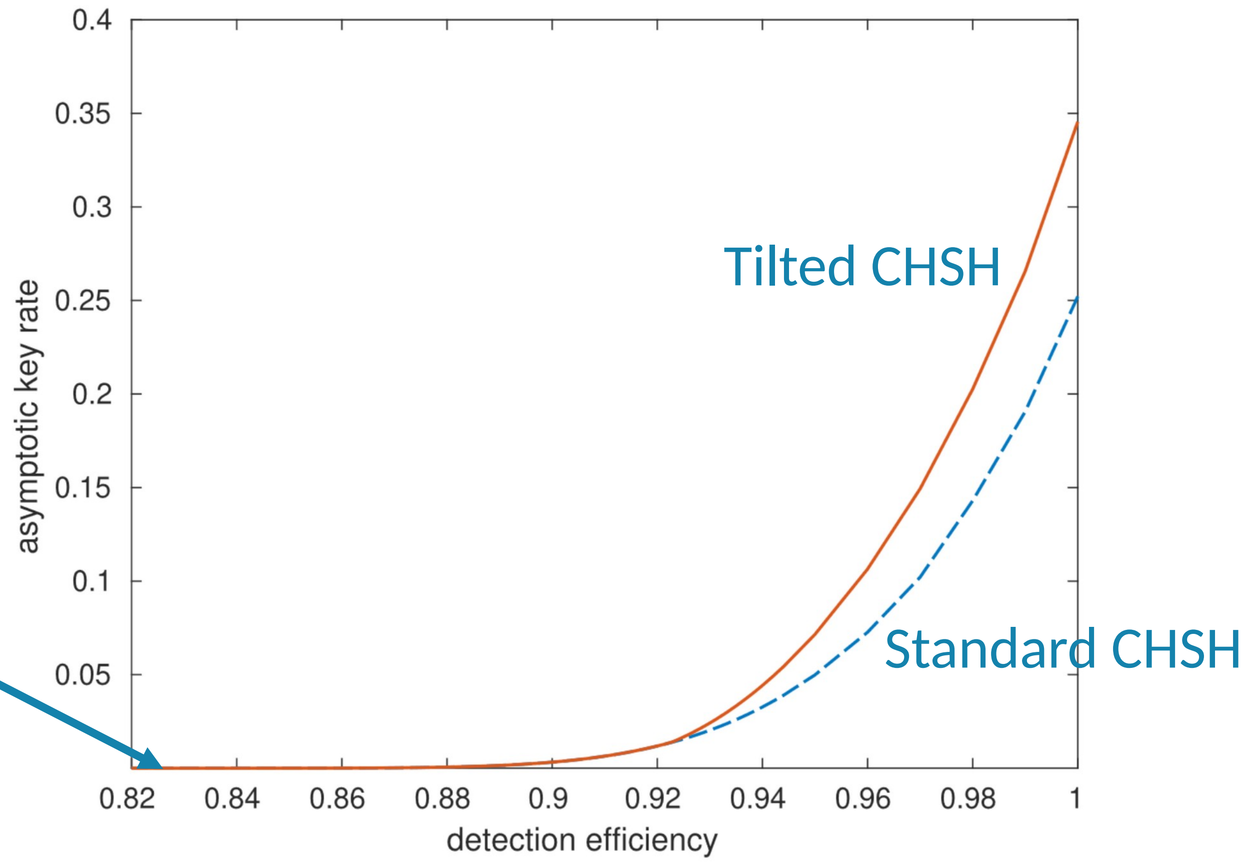
- Alternative view: using two statistics
- : Closed-form keyrate expression
- : Numerical approach
  - New(?) continuity bound!

More efficient approach in [WAP20] arXiv:2007.16146

Results: SPDC (photon) model

- Tilted CHSH improves keyrate

- But threshold remains similar
  - (About 82.6%)



Combining variants [TSB+20]

- Noisy preprocessing + random key measurements + all statistics
- Numerical, but *reliable*
  - Also: converges to tight bound
- Minimization over states
  - Follow [WLC17] arXiv:1710.05511
- Minimization over measurements
  - Use continuity bound + other tricks

min

over states and measurements

Results: depolarizing noise

Protocol	Noise threshold
[PAB+09] “Basic” protocol	7.14%
[HST+20] Noisy preprocessing	8.08%
[WAP20] Noisy preprocessing + tilted CHSH	8.34%
[SGP+20] Random key measurements	8.39%
[TSB+20] Combining variants	9.33%
Simple upper bound for this family	9.57%

Results: existing Bell experiments

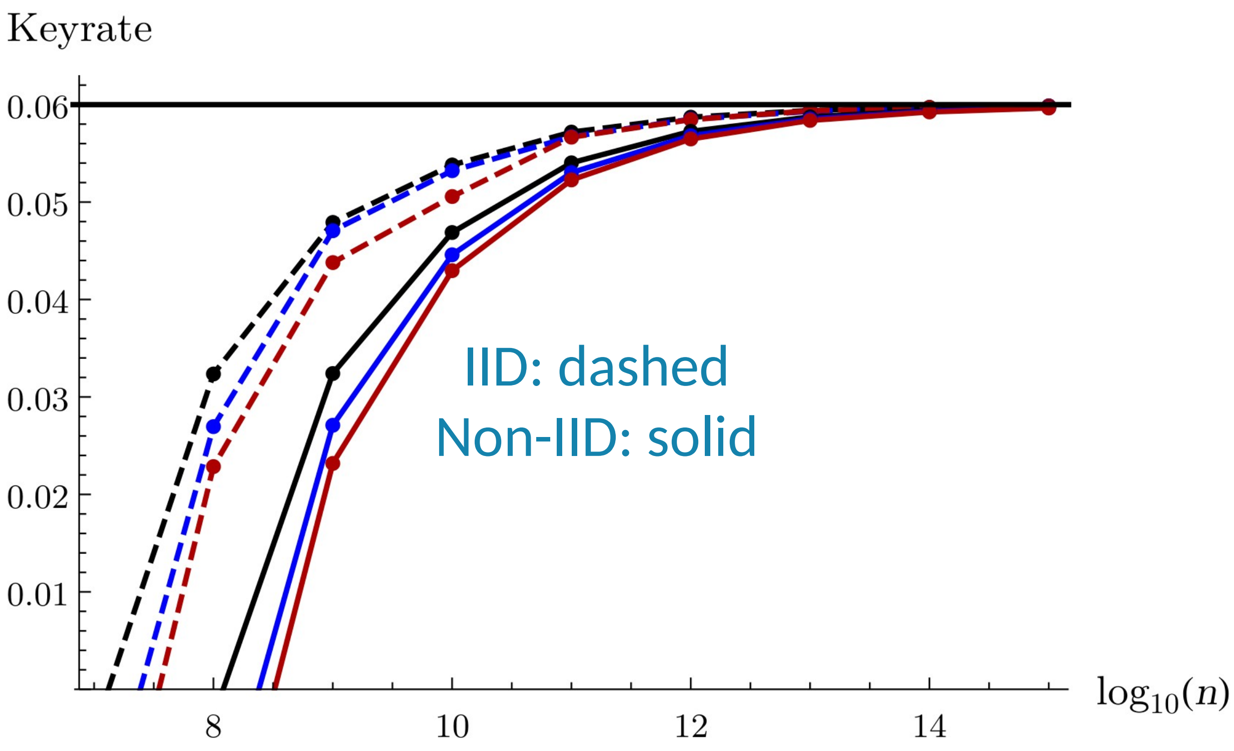
- Asymptotic keyrates > 0 (as expected)
- NV centres, cold atoms:
  - Mainly via random key measurements (+ a bit of noisy preprocessing)
- Photons (SPDC)
  - Optimizing experiment is challenging
  - Did not find improvements beyond [SBV+20] (noisy preprocessing)

Part 2: Finite-size analysis [TSB+20]

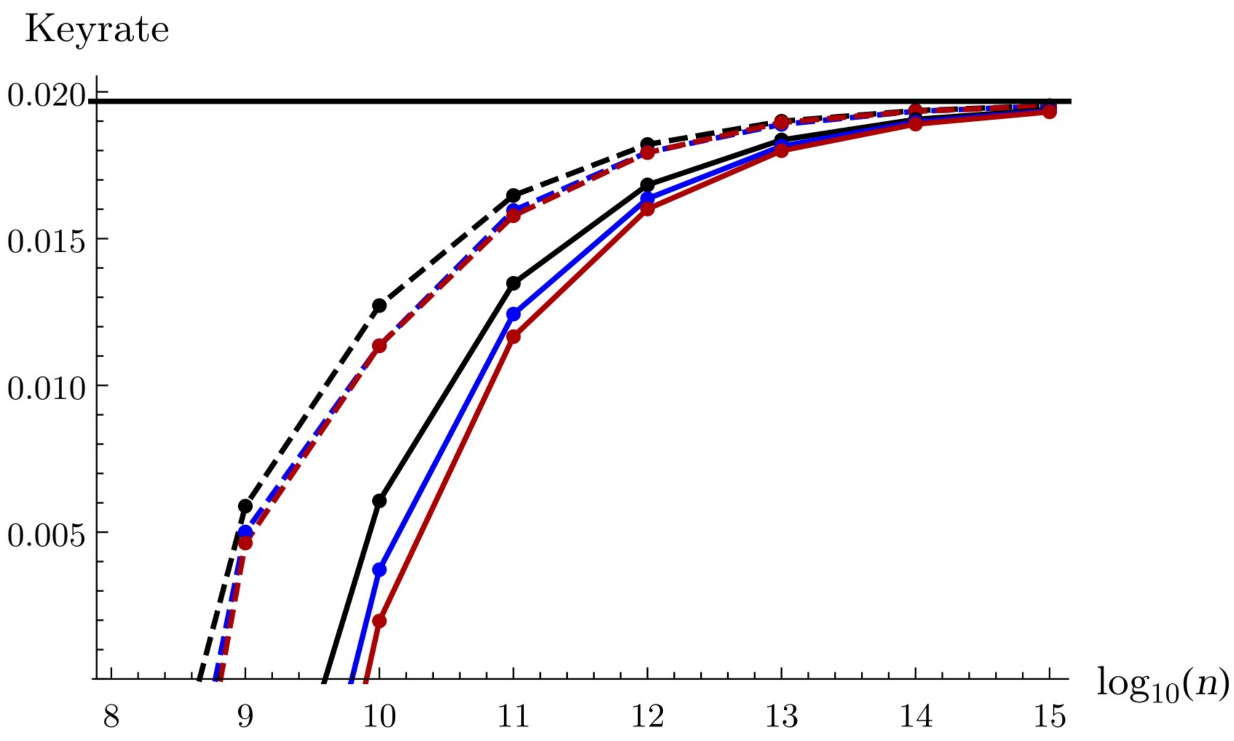
- Using entropy accumulation theorem
  - Incorporates finite-size and non-IID effects
  - Previously applied to “basic” protocol [AFRV16] arXiv:1607.01797

- Our technical contributions:
  - Combining protocol variants
  - Proof modifications (tighter bounds, practical error correction)
  - Pre-shared key proposal (2x keyrate for random key measurements)

Finite-size bounds

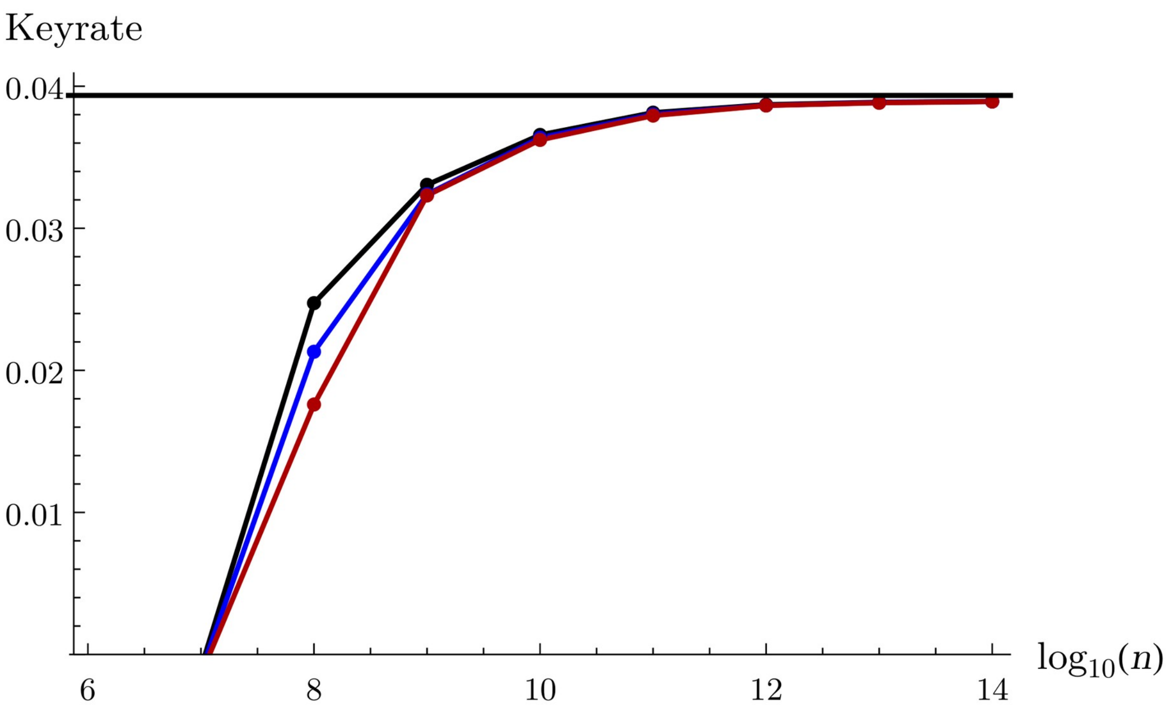


NV-centre Bell test [HBD+15]



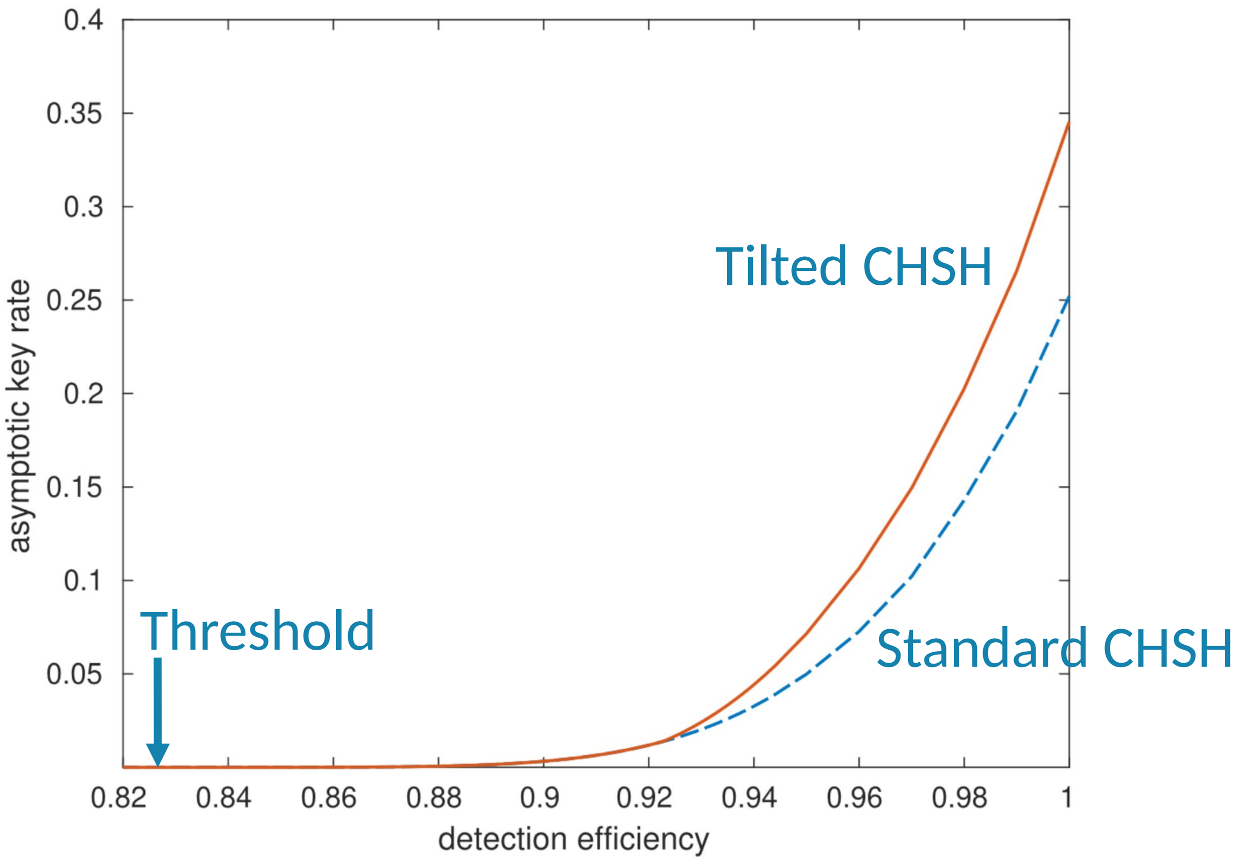
Cold-atom Bell test [RBG+17]

Finite-size bounds (optimized for IID)



Cold-atom Bell test [RBG+17]

Recap: SPDC model (asymptotic)



Subsequent developments

- Better methods to compute asymptotic keyrates
  - [BFF21] arxiv:2106.13692 and [MPW21] arxiv:2107.08894
- Simplified photonic model:
  - Threshold efficiency 80.26%
  - Substantially higher keyrates
- No finite-size analysis yet

Summary and outlook

- Our contributions
  - Method for tilted CHSH (see independent work [WAP20])
  - Method for combining all variants
  - New depolarizing-noise threshold
  - Various improvements to finite-size analysis
- Going forward
  - NV centres / cold atoms need significant improvement
  - Photonic implementations promising; need detailed analysis
  - Upper bounds: [KWW18] [WDH19] [AL20] [CFH20] [FBJL+21] [KHD21]

Thank you!