Multi-partite entanglement can speed up quantum key distribution in networks

M. Epping, H. Kampermann, C. Macchiavello, and *D. Bruß*

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Germany

SPONSORED BY THE

Federal Ministry of Education and Research

European Commission

ISNFQC18 Kolkata, 29th Jan 2018

Outline

- Entangled-based quantum key distribution (QKD)

Outline

- Entanglement-based quantum key distribution (QKD)
- Generalisation to many users (conference key agreement)

Outline

- Entanglement-based quantum key distribution (QKD)
- Generalisation to many users (conference key agreement)
- Advantage of multipartite entanglement in quantum networks

Outline

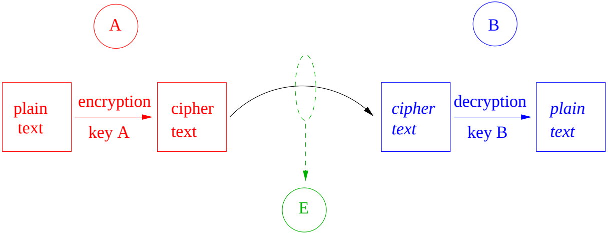
- Entanglement-based quantum key distribution (QKD)
- Generalisation to many users (conference key agreement)
- Advantage of multipartite entanglement in quantum networks

Outline

- Entanglement-based quantum key distribution (QKD)
- Generalisation to many users (conference key agreement)
- Advantage of multipartite entanglement in quantum networks

M. Epping, H. Kampermann, C. Macchiavello, and DB, New J. Phys. **19**, *093012 (2017)*

Quantum key distribution (QKD)



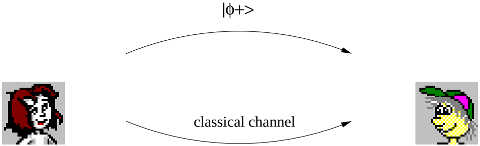
Vernam cipher ≡ "one-time pad" (1917):
Encoding with secret random key (only known to Alice and Bob, not to Eve). Proven to be secure.

How to establish secret random key?
↪ quantum cryptography ≡ quantum key distribution (QKD)

Entanglement-based QKD (between two parties)

A. Ekert, Phys. Rev. Lett. **67**, *661 (1991)*

Aim: secret random key for Alice and Bob



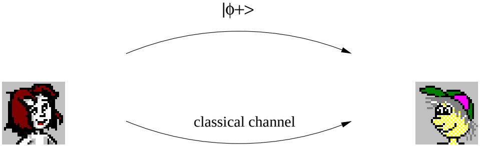
1) A sends half of a Bell state to Bob: $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$
   A and B measure, use 2 bases randomly: $\uparrow\!\!\!\rightarrow$ or $\searrow\!\nearrow$
2) A and B exchange class. info about basis,
   keep matching cases: $1 \quad r \quad 0 \quad 0 \quad 1 \quad r \quad 0 \quad r$

$\hookrightarrow$ Alice and Bob have established secret random key!

Entanglement-based QKD (between two parties)

A. Ekert, Phys. Rev. Lett. **67**, *661 (1991)*

Aim: secret random key for Alice and Bob



1) A sends half of a Bell state to Bob: $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$
A and B measure, use 2 bases randomly: ↕↔ or ⤡⤢

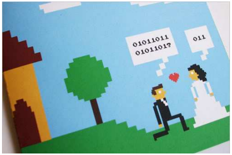
2) A and B exchange class. info about basis,
keep matching cases: $1 \;\; r \;\; 0 \;\; 0 \;\; 1 \;\; r \;\; 0 \;\; r$

$\hookrightarrow$ Alice and Bob have established secret random key!

Security: monogamy of entanglement

Monogamy of entanglement

V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, *052306 (2000)*



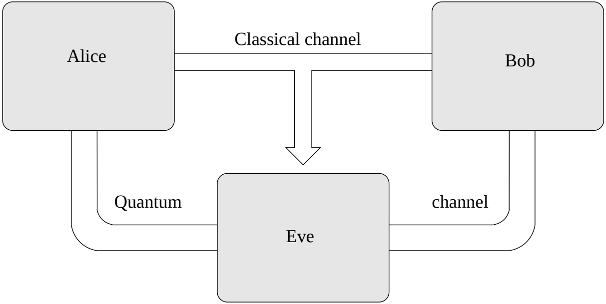
Impossible!

Possible

$$E(B|A) + E(B|C) \leq E(B|AC)$$

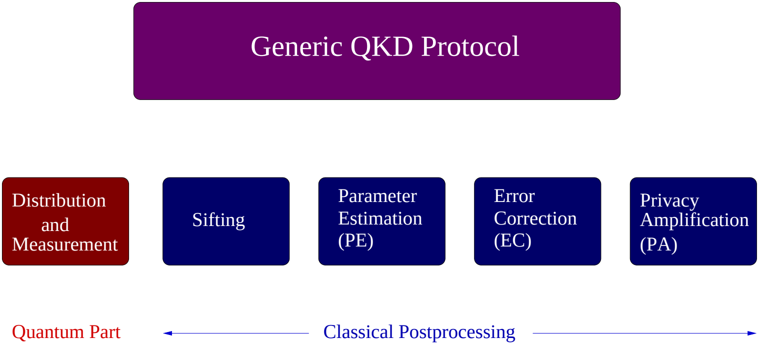
QKD in reality: noisy entangled state, $\rho = p|\phi^+\rangle\langle\phi^+| + (1-p)\frac{1}{4}\mathbb{1}$,
assume Eve to have purifying state (is partially correlated with A/B)
$\hookrightarrow$ security analysis

Quantum Key Distribution (QKD)

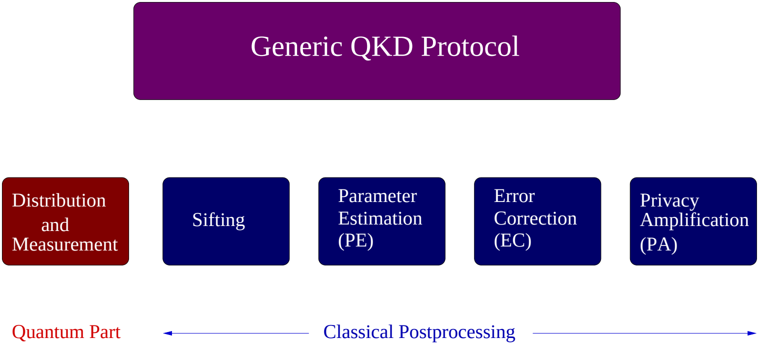


- Scenario: Alice und Bob have quantum channel (controlled by Eve) and classical channel (authenticated)
- Secure communication ⇔ Creation of a secret random key pair between Alice and Bob
- No restrictions on Eve

QKD: General description of a QKD protocol



QKD: General description of a QKD protocol



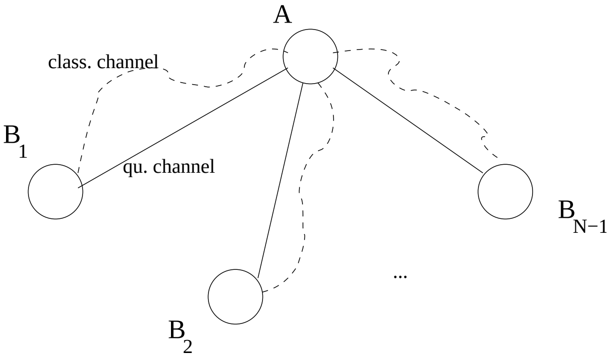
Equivalence of prepare+measure QKD with entanglement-based QKD

$\hookrightarrow$ In the following: use entanglement-based scheme

Generalisation of QKD to more than two parties

M. Epping, H. Kampermann, C. Macchiavello, and DB, New J. Phys. **19**, *093012 (2017)*

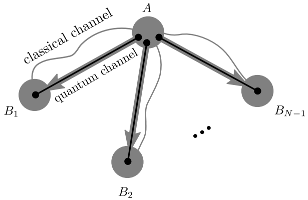
Aim: establish joint secret random key between N parties,
i.e. "conference key"



Establishing a conference key: Two possibilities

M. Epping, H. Kampermann, C. Macchiavello, and DB, New J. Phys. **19**, *093012 (2017)*

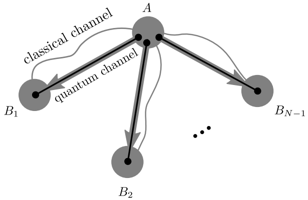
Using bipartite entanglement (2QKD):



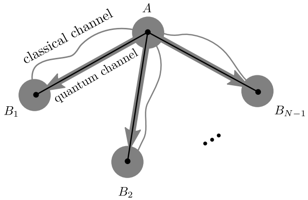
Establishing a conference key: Two possibilities

M. Epping, H. Kampermann, C. Macchiavello, and DB, New J. Phys. **19**, *093012 (2017)*

Using bipartite entanglement (2QKD):



... or using multipartite entanglement (NQKD):



Multipartite entanglement

Multipartite entanglement

Multipartite entanglement of composite (pure) states of N parties:

$$|\psi\rangle = |a\rangle_{1,\ldots,k} \otimes |b\rangle_{k+1,\ldots,N} \quad \hookrightarrow \quad \text{separable across bipartite split}$$
$$|\psi\rangle \neq |a\rangle_{1,\ldots,k} \otimes |b\rangle_{k+1,\ldots,N} \quad \hookrightarrow \quad \text{multipartite entangled}$$

Multipartite entanglement

Multipartite entanglement of composite (pure) states of N parties:

$$|\psi\rangle = |a\rangle_{1,...,k} \otimes |b\rangle_{k+1,...,N} \hookrightarrow$$ separable across bipartite split

$$|\psi\rangle \neq |a\rangle_{1,...,k} \otimes |b\rangle_{k+1,...,N} \hookrightarrow$$ multipartite entangled

Example (separable): $|\psi\rangle = |0\rangle|0\rangle...|0\rangle$

Example (entangled): GHZ states of N qubits

$$|\psi_j^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|j\rangle \pm |1\rangle|\bar{j}\rangle)$$

where j takes values $0, ..., 2^{N-1} - 1$ in binary notation;
$\bar{j}$ is negation of j, e.g. if $j = 010$ then $\bar{j} = 101$

Multipartite entanglement for QKD

Which types of multipartite entanglement can be used for QKD?

Multipartite entanglement for QKD

Which types of multipartite entanglement can be used for QKD?

Theorem (Perfect resource state for multipartite QKD)

For N qubits, with $N \geq 3$, the state
$|\phi_{corr}\rangle = a_{0,...,0}|0,...,0\rangle + a_{1,...,1}|1,...,1\rangle$ with $|\, a_{0,...,0}\,|^2 + |\, a_{1,...,1}\,|^2 = 1$
leads to perfect classical correlations between any number of parties, if and only if each of them measures in the z-basis.

Multipartite entanglement for QKD

Which types of multipartite entanglement can be used for QKD?

Theorem (Perfect resource state for multipartite QKD)

For N qubits, with $N \geq 3$, the state
$|\phi_{corr}\rangle = a_{0,\dots,0}|0,\dots,0\rangle + a_{1,\dots,1}|1,\dots,1\rangle$ with $|\,a_{0,\dots,0}\,|^2 + |\,a_{1,\dots,1}\,|^2 = 1$
leads to perfect classical correlations between any number of parties, if and only if each of them measures in the z-basis.

Proof: "$\Leftarrow$" clear;
"$\Rightarrow$": observable $\mathcal{M}_{ij}$ of two parties i and j:

$$\mathcal{M}_{ij} = (\vec{M}_i \cdot \vec{\sigma}) \otimes (\vec{M}_j \cdot \vec{\sigma}) = \sum_{\alpha,\beta \in \{x,y,z\}} M_i^\alpha M_j^\beta \sigma_i^\alpha \otimes \sigma_j^\beta,$$

$$\langle \phi_{corr}|\sigma_i^\alpha \otimes \sigma_j^\beta|\phi_{corr}\rangle = 0 \;\; \text{unless} \;\; \alpha = \beta = z,$$

also $\langle \phi_{corr}|\sigma_i^\alpha \otimes \sigma_j^\beta|\phi_{corr}\rangle = 2[p_i^\alpha(+)p_j^\beta(+) + p_i^\alpha(-)p_j^\beta(-)] - 1$,
thus $p_i^\alpha(+)p_j^\beta(+) + p_i^\alpha(-)p_j^\beta(-) \neq 1$, unless $\alpha = \beta = z$.

Multipartite QKD protocol

If one requires perfect correlations and uniformity of key,
the *only* possible resource state is $|GHZ\rangle = \frac{1}{\sqrt{2}}(|0,...,0\rangle + |1,...,1\rangle)$.

Multipartite QKD protocol

If one requires perfect correlations and uniformity of key,
the *only* possible resource state is $|GHZ\rangle = \frac{1}{\sqrt{2}}(|0,...,0\rangle + |1,...,1\rangle)$.

Protocol for N-party quantum conference key distribution (NQKD):

Multipartite QKD protocol

If one requires perfect correlations and uniformity of key,
the *only* possible resource state is $|GHZ\rangle = \frac{1}{\sqrt{2}}(|0, ..., 0\rangle + |1, ..., 1\rangle)$.

Protocol for N-party quantum conference key distribution (NQKD):

1) *State preparation:* Parties A and B_i, $i = 1, 2, ..., N-1$ share $|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right)$.

Multipartite QKD protocol

If one requires perfect correlations and uniformity of key,
the *only* possible resource state is $|GHZ\rangle = \frac{1}{\sqrt{2}}(|0,...,0\rangle + |1,...,1\rangle)$.

Protocol for N-party quantum conference key distribution (NQKD):

1) *State preparation:* Parties A and B_i, $i = 1, 2, ..., N-1$ share $|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right)$.
2) *Measurement:* First type of measurement: All parties measure their respective qubits in z-basis. Second type: parties measure randomly, with equal probability, in x- or y-basis (much less frequent).

Multipartite QKD protocol

If one requires perfect correlations and uniformity of key,
the *only* possible resource state is $|GHZ\rangle = \frac{1}{\sqrt{2}}(|0,...,0\rangle + |1,...,1\rangle)$.

Protocol for N-party quantum conference key distribution (NQKD):

1) *State preparation:* Parties A and B_i, $i = 1, 2, ..., N-1$ share $|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right)$.
2) *Measurement:* First type of measurement: All parties measure their respective qubits in z-basis. Second type: parties measure randomly, with equal probability, in x- or y-basis (much less frequent).
3) *Parameter estimation:* Parties use equal number of randomly chosen rounds of first and second type to estimate the error rates.

Multipartite QKD protocol

If one requires perfect correlations and uniformity of key,
the *only* possible resource state is $|GHZ\rangle = \frac{1}{\sqrt{2}}(|0,...,0\rangle + |1,...,1\rangle)$.

Protocol for N-party quantum conference key distribution (NQKD):

1) *State preparation:* Parties A and B_i, $i = 1, 2, ..., N-1$ share $|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}\right)$.
2) *Measurement:* First type of measurement: All parties measure their respective qubits in z-basis. Second type: parties measure randomly, with equal probability, in x- or y-basis (much less frequent).
3) *Parameter estimation:* Parties use equal number of randomly chosen rounds of first and second type to estimate the error rates.
4) *Classical post-processing:* As in the bipartite protocol, error correction and privacy amplification is performed.

Secret key rate for NQKD

Security analysis:

- Analogous to bipartite case, with modifications in worst-case error correction and depolarisation

  R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A 72, 012332 (2005)

Secret key rate for NQKD

Security analysis:

- Analogous to bipartite case, with modifications in worst-case error correction and depolarisation

  R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A 72, 012332 (2005)

- Figure of merit: secret fraction,
  i.e. ratio of secret bits and number of shared states r_∞:

Secret key rate for NQKD

Security analysis:

- Analogous to bipartite case, with modifications in worst-case error correction and depolarisation

  R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A 72, 012332 (2005)

- Figure of merit: secret fraction,
  i.e. ratio of secret bits and number of shared states r_∞:

$$r_\infty = \sup_{U \leftarrow K} \inf_{\sigma_{A\{B_i\}} \in \Gamma} [S(U|E) - \max_{i \in \{1,\ldots N-1\}} H(U|K_i)],$$

with $U \leftarrow K$: bitwise preprocessing channel on A's raw key bit K,
$S(U|E)$: conditional von-Neumann entropy of (class.) key variable and E,
$H(U|K_i)$: conditional Shannon entropy of U and B_i's guess of it,

Γ: set of all density matrices $\sigma_{A\{B_i\}}$ of A and B_i consistent with parameter estimation

Secret key rate: $R = r_\infty R_{\text{rep}}$ with repetition rate R_{rep}

Secret key rate for NQKD

Introduce (extended) depolarisation procedure, $\hookrightarrow$ GHZ-diagonal state
$\hookrightarrow$ calculate secret fraction r_∞:

Secret key rate for NQKD

Introduce (extended) depolarisation procedure, $\hookrightarrow$ GHZ-diagonal state $\hookrightarrow$ calculate secret fraction r_∞:

$$
\begin{aligned}
r_\infty = \quad & \left(1 - \frac{Q_Z}{2} - Q_X\right) \log_2 \left(1 - \frac{Q_Z}{2} - Q_X\right) \\
& + \left(Q_X - \frac{Q_Z}{2}\right) \log_2 \left(Q_X - \frac{Q_Z}{2}\right) \\
& + (1 - Q_Z)(1 - \log_2(1 - Q_Z)) - h(\max_{1 \le i \le N-1} Q_{AB_i})
\end{aligned}
$$

with Q_Z: probability that at least one B_i obtains different result than A in z-measurement,
with Q_X: probability that at least one B_i obtains in x-measurement a result that is incompatible with noiseless state,
binary entropy: $h(p) = -p \log_2 p - (1-p) \log_2 (1-p)$,

Q_{AB_i}: probability that z-measurements of A and B_i disagree.

Example for explicit key rates

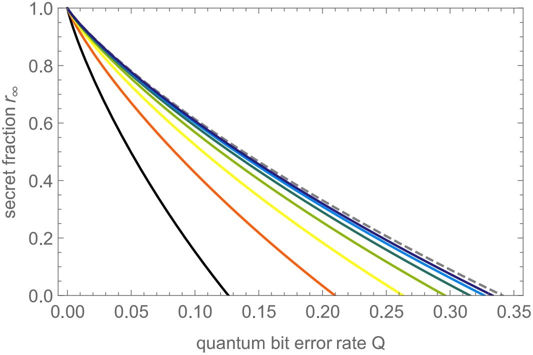
Noise model: mixture of GHZ-state and white noise (then $Q = Q_z$)

$$r_\infty(Q,N) = 1 + h(Q) - h\left(Q\frac{2^N-1}{2^N-2}\right) - h\left(Q\frac{2^{N-1}}{2^N-2}\right) + \left(\log_2(2^{N-1}-1) - \frac{2^N-1}{2^N-2}\log_2(2^N-1)\right)Q,$$

Example for explicit key rates

Noise model: mixture of GHZ-state and white noise (then $Q = Q_z$)

$$r_\infty(Q,N) = 1 + h(Q) - h\left(Q\frac{2^N-1}{2^N-2}\right) - h\left(Q\frac{2^{N-1}}{2^N-2}\right) + \left(\log_2(2^{N-1}-1) - \frac{2^N-1}{2^N-2}\log_2(2^N-1)\right)Q,$$



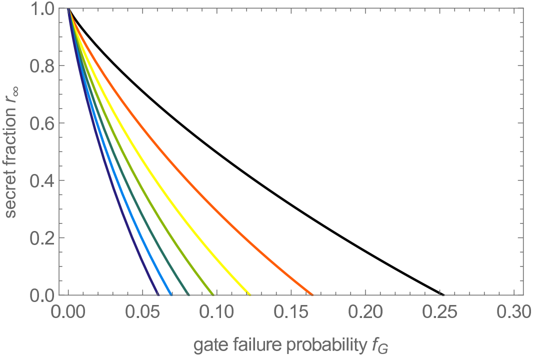
Key rates for $N = 2, 3, ..., 8$, from left to right.

Secret key rate as function of gate failure probability

Consider imperfect state preparation (depolarising noise): experimental creation of GHZ-state is more demanding with higher N!

Secret key rate as function of gate failure probability

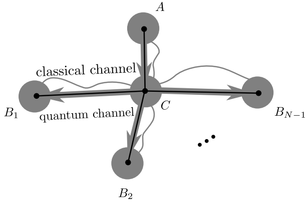
Consider imperfect state preparation (depolarising noise): experimental creation of GHZ-state is more demanding with higher N!



Key rates for $N = 2, 3, ..., 8$, from right to left.

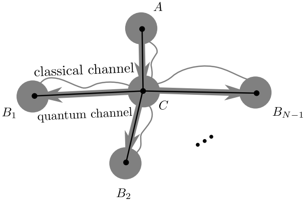
Advantage of NQKD in quantum networks

Consider quantum networks with routers (can produce and entangle qubits), fixed channel capacity:

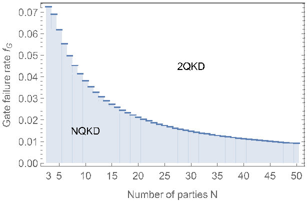


Advantage of NQKD in quantum networks

Consider quantum networks with routers (can produce and entangle qubits), fixed channel capacity:



For small gate failure probability: NQKD is better than 2QKD!



Connection to quantum network coding

Processing of data at intermediate network nodes can improve throughput and increase robustness of quantum network with bottleneck.

Connection to quantum network coding

Processing of data at intermediate network nodes can improve throughput and increase robustness of quantum network with bottleneck.

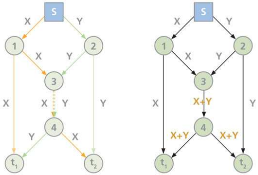
Famous example - the butterfly network:

Connection to quantum network coding

Processing of data at intermediate network nodes can improve throughput and increase robustness of quantum network with bottleneck.

Famous example - the butterfly network:

Classical network coding:

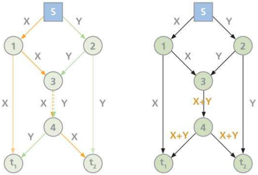


Connection to quantum network coding

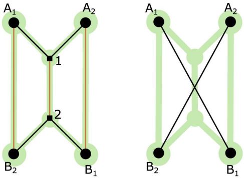
Processing of data at intermediate network nodes can improve throughput and increase robustness of quantum network with bottleneck.

Famous example - the butterfly network:

Classical network coding:



Quantum network coding:

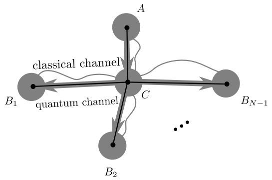


(a)Pre-measurement state. (b)Post-measurement state.

M. Epping, H. Kampermann, and DB, New J. Phys. **18**, *103052 (2016)*

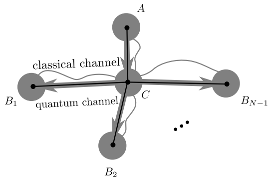
Connection to quantum network coding

Distribution of GHZ-state in above network, with quantum operations at node C (router), and fixed channel capacities for all links:



Connection to quantum network coding

Distribution of GHZ-state in above network, with quantum operations at node C (router), and fixed channel capacities for all links:



- A produces Bell state and sends only one qubit C to router: $|\text{—}\rangle_{CA} = \frac{1}{\sqrt{2}}(|0+\rangle + |1-\rangle)_{CA}$
- C produces $(N-1)$ qubits and entangles them with C via C_z gates: $|\psi_{\text{total}}\rangle = \frac{1}{\sqrt{2}}(|+\rangle_C |GHZ'\rangle_{AB_i} + |-\rangle_C X_{B_1} |GHZ'\rangle_{AB_i})$ where $|GHZ'\rangle$ is GHZ-state in X-basis.
- Router measures qubit C in X-basis and distributes qubits to B_i.
- Impossible to create $(N-1)$ Bell pairs by sending single qubit from A to router; need $(N-1)$ network uses.

M. Epping, H. Kampermann, and DB, New J. Phys. **18**, *103052 (2016)*

Summary and open questions

- Monogamy of entanglement $\hookrightarrow$ security in entanglement-based QKD

Summary and open questions

- Monogamy of entanglement $\hookrightarrow$ security in entanglement-based QKD
- Generalisation to multiparty QKD

Summary and open questions

- Monogamy of entanglement $\hookrightarrow$ security in entanglement-based QKD
- Generalisation to multiparty QKD
- Secret key rate as function of number of parties and noise

Summary and open questions

- Monogamy of entanglement $\hookrightarrow$ security in entanglement-based QKD
- Generalisation to multiparty QKD
- Secret key rate as function of number of parties and noise
- Comparison for 2QKD and NQKD in quantum networks with routers: multipartite entanglement can lead to advantage

Summary and open questions

- Monogamy of entanglement $\hookrightarrow$ security in entanglement-based QKD
- Generalisation to multiparty QKD
- Secret key rate as function of number of parties and noise
- Comparison for 2QKD and NQKD in quantum networks with routers: multipartite entanglement can lead to advantage
- Experimental implementation of NQKD?

Summary and open questions

- Monogamy of entanglement $\hookrightarrow$ security in entanglement-based QKD
- Generalisation to multiparty QKD
- Secret key rate as function of number of parties and noise
- Comparison for 2QKD and NQKD in quantum networks with routers: multipartite entanglement can lead to advantage
- Experimental implementation of NQKD?
- Starting from other states with less than perfect correlations? Finite key analysis? Device-independent scenario?

Summary and open questions

- Monogamy of entanglement $\hookrightarrow$ security in entanglement-based QKD
- Generalisation to multiparty QKD
- Secret key rate as function of number of parties and noise
- Comparison for 2QKD and NQKD in quantum networks with routers: multipartite entanglement can lead to advantage
- Experimental implementation of NQKD?
- Starting from other states with less than perfect correlations? Finite key analysis? Device-independent scenario?

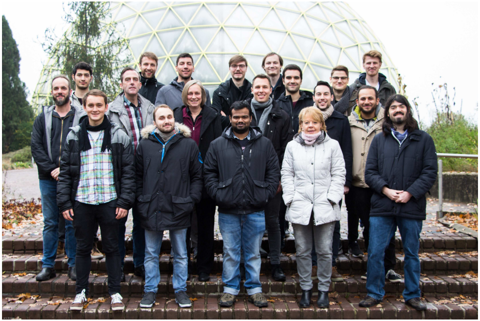
Summary and open questions

- Monogamy of entanglement $\hookrightarrow$ security in entanglement-based QKD
- Generalisation to multiparty QKD
- Secret key rate as function of number of parties and noise
- Comparison for 2QKD and NQKD in quantum networks with routers: multipartite entanglement can lead to advantage
- Experimental implementation of NQKD?
- Starting from other states with less than perfect correlations? Finite key analysis? Device-independent scenario?

M. Epping, H. Kampermann, C. Macchiavello, and DB, New J. Phys. **19**, *093012 (2017)*

Quantum Information Theory in Düsseldorf

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Germany



from left to right: J. Bremer, J. M. Henning, D. Miller, H. Kampermann, T. Holz, G. Gianfelici, M. Zibull, DB, T. Backhausen, S. Datta, F. Bischof, T. Wagner, C. Liorni, C. Glowacki, F. Grasselli, C. Hoffmeister, B. Sanvee, L. Tendick, M. Battiato

SPONSORED BY THE
Federal Ministry of Education and Research

Deutsche Forschungsgemeinschaft DFG

European Commission

HEINRICH HEINE UNIVERSITÄT DÜSSELDORF