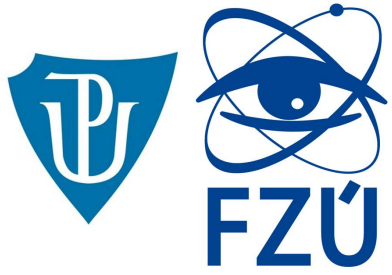
Quantum cryptography for socio-economic problems



Kishore Thapliyal

Joint Laboratory of Optics of Palacky University and Institute of Physics of Academy of Science of the Czech Republic, Olomouc, Czech Republic

QIPA 2018,
HRI Allahabad
December 05, 2018

Quantum cryptography for socio-economic problems

Kishore Thapliyal

Jaypee Institute of Information Technology,
Noida, India

QIPA 2018,
HRI Allahabad

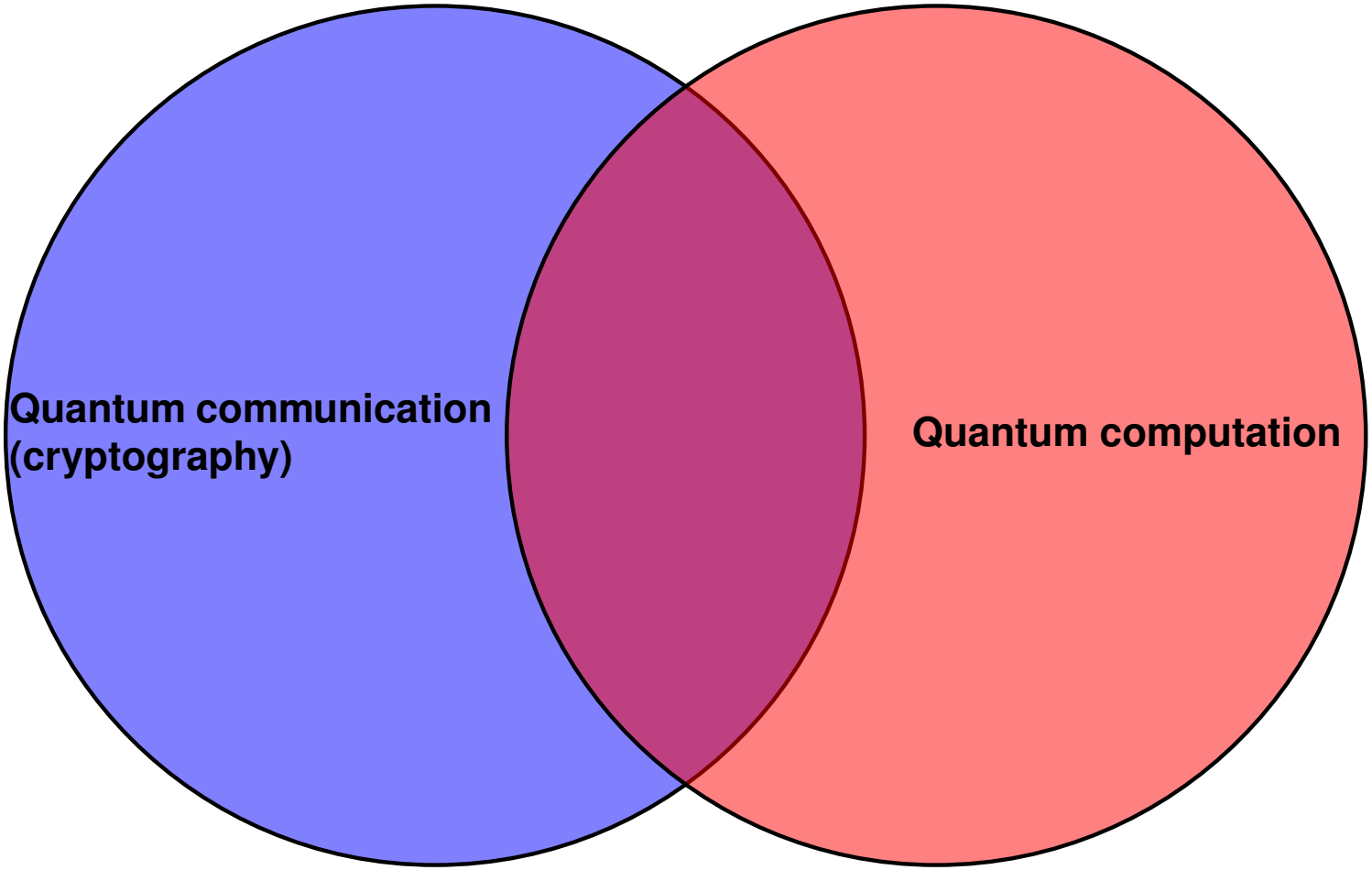
December 05, 2018

Outline

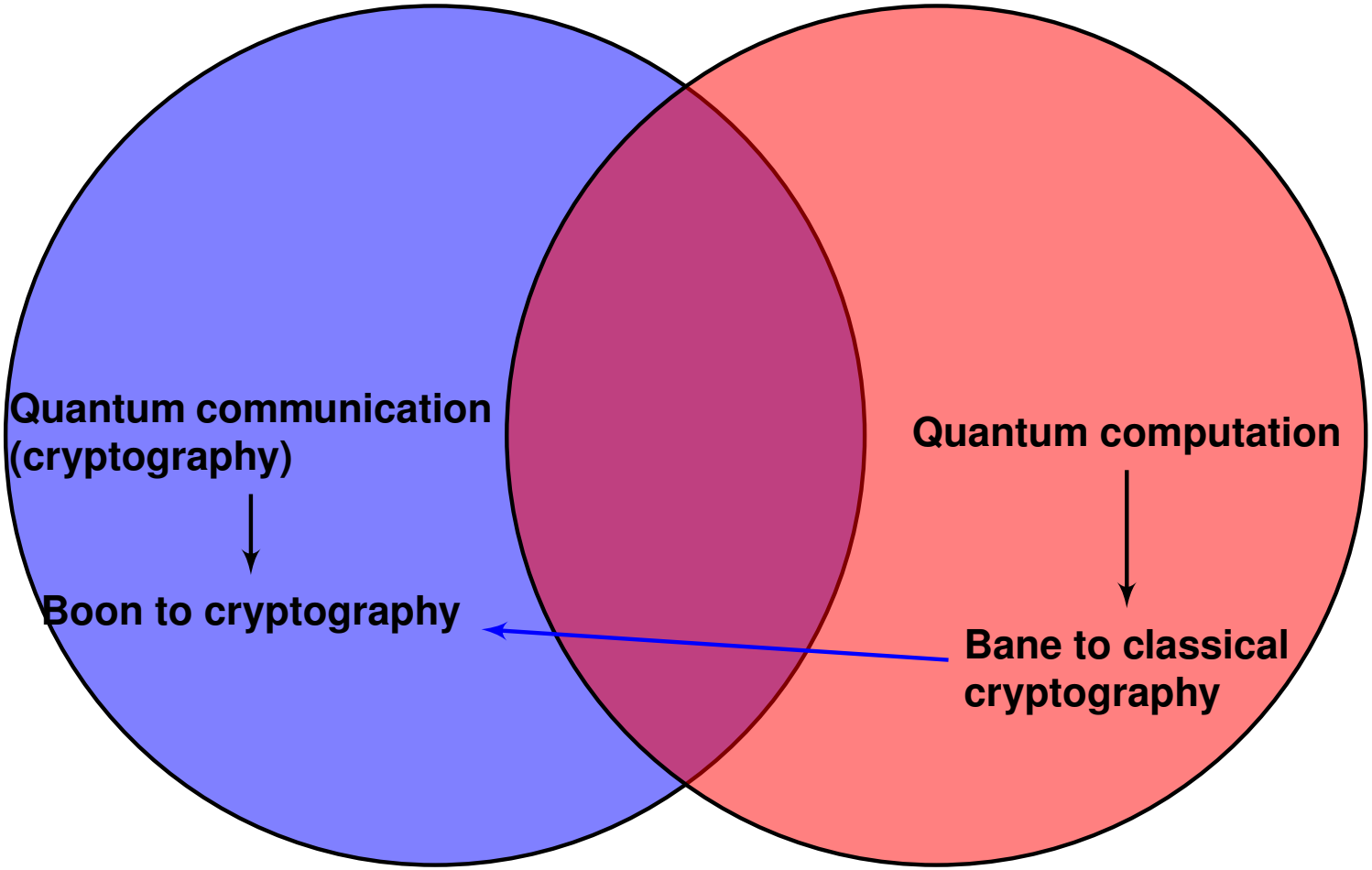
1. Quantum information processing: Quantum communication and computation
2. Secure multiparty computation
3. Quantum solutions for socio-economic problems

Outline

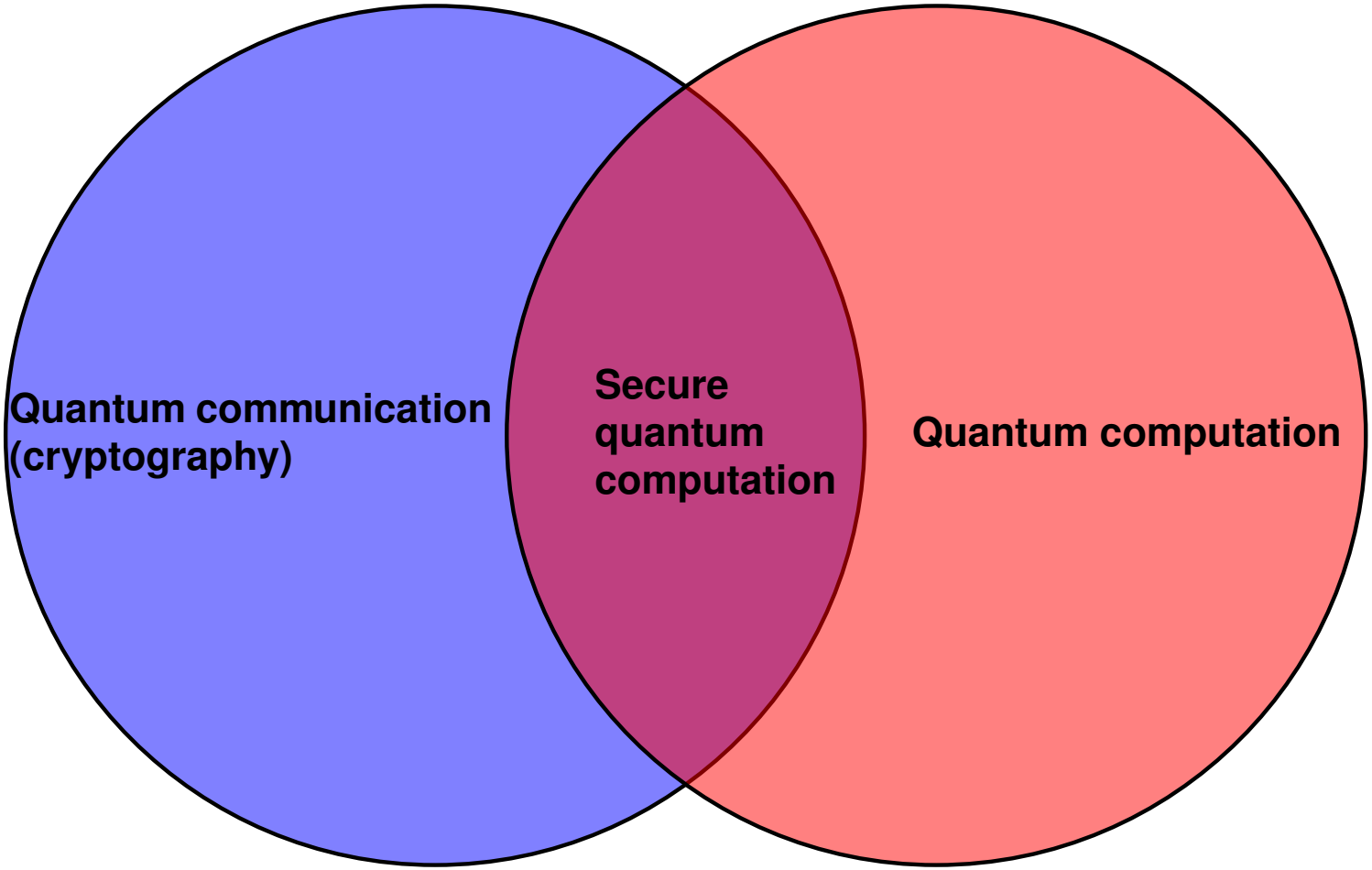
Quantum information processing: Boon or bane?



Quantum information processing: Boon or bane?

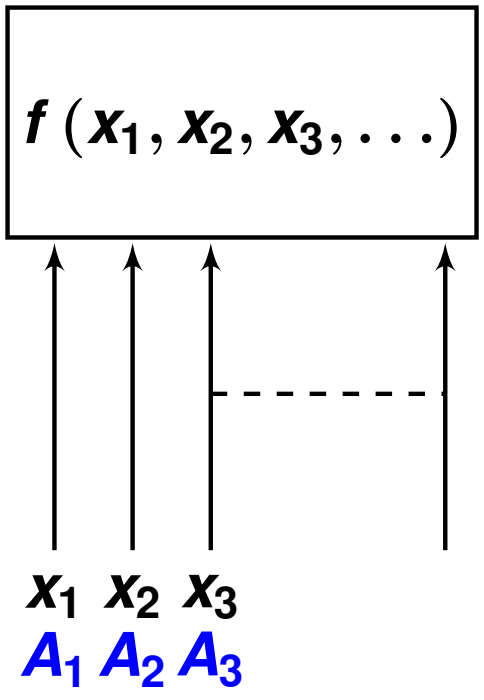


Quantum information processing: Boon or bane?

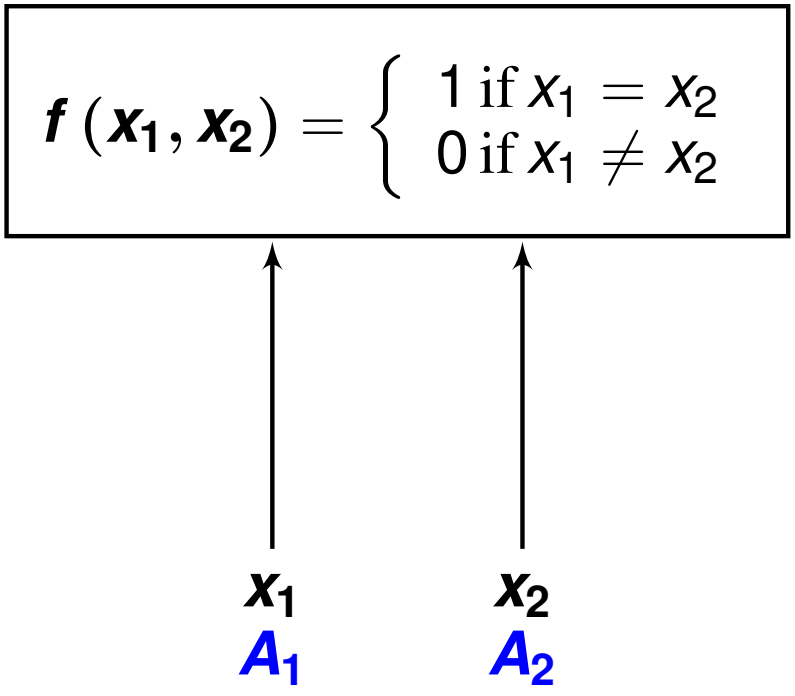


Outline

Idea of secure computation



Example: Quantum private comparison/ Socialist millionaire problem

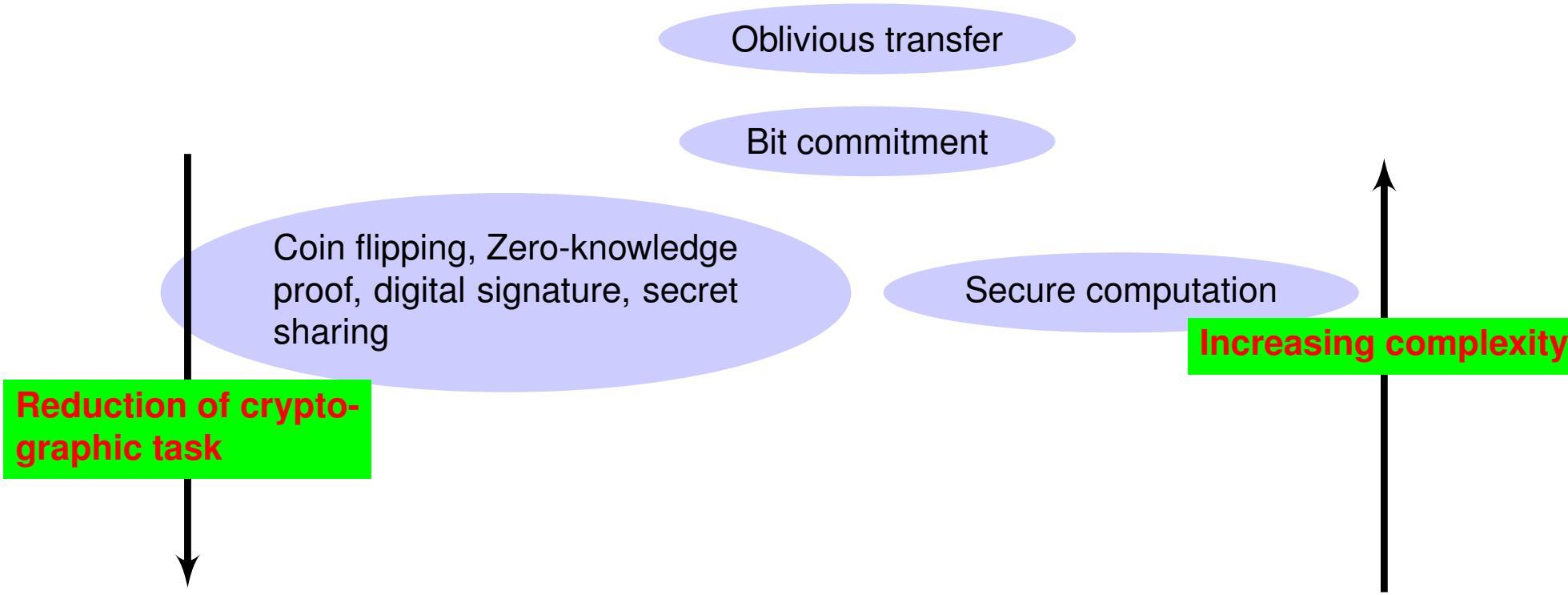


Secure computation in real life scenarios

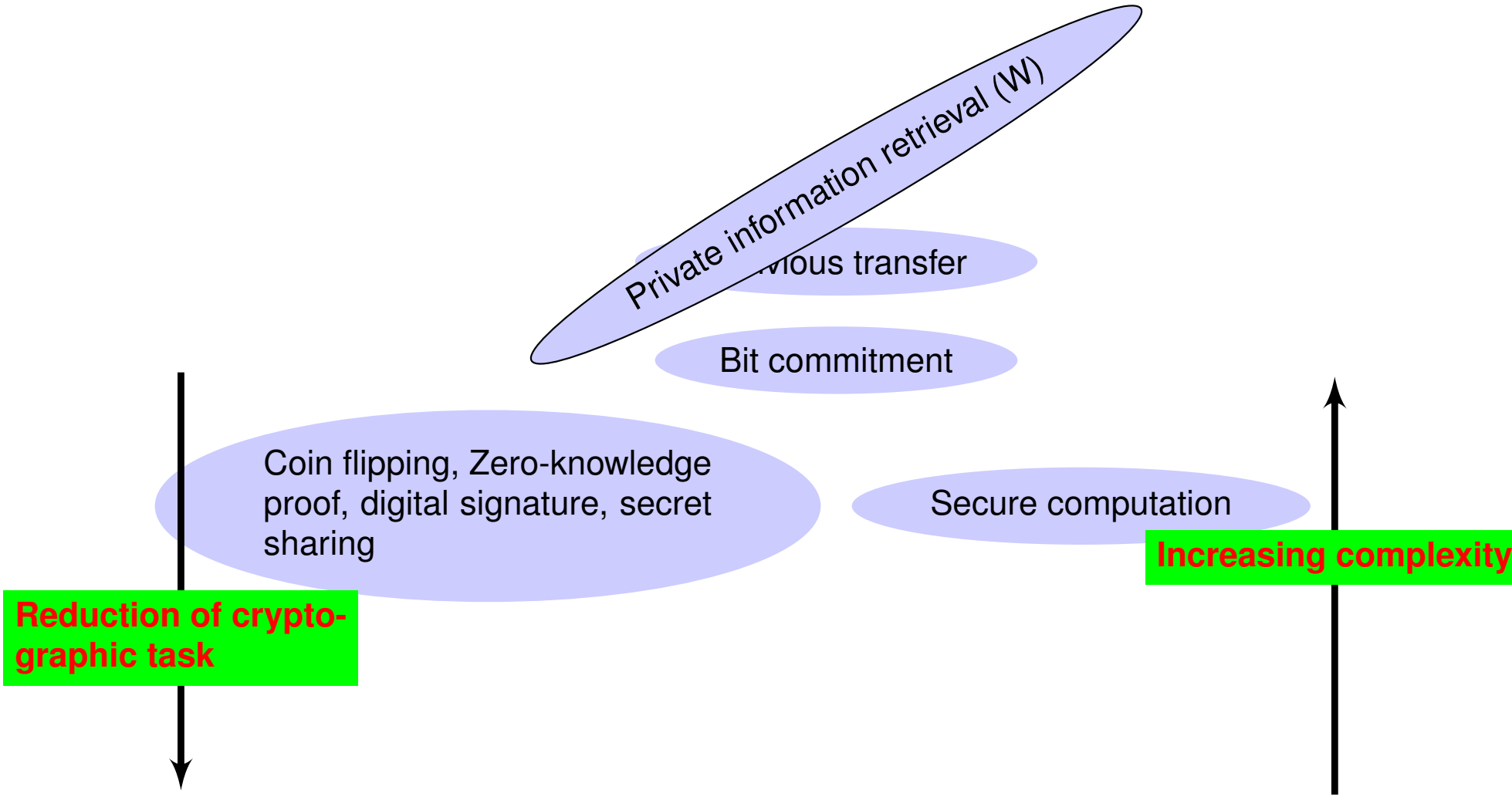
Private information retrieval

Also, in secure supply chain collaboration, as a countermeasure against (mainly hardware) side-channel attacks, and to avoid satellite collisions.

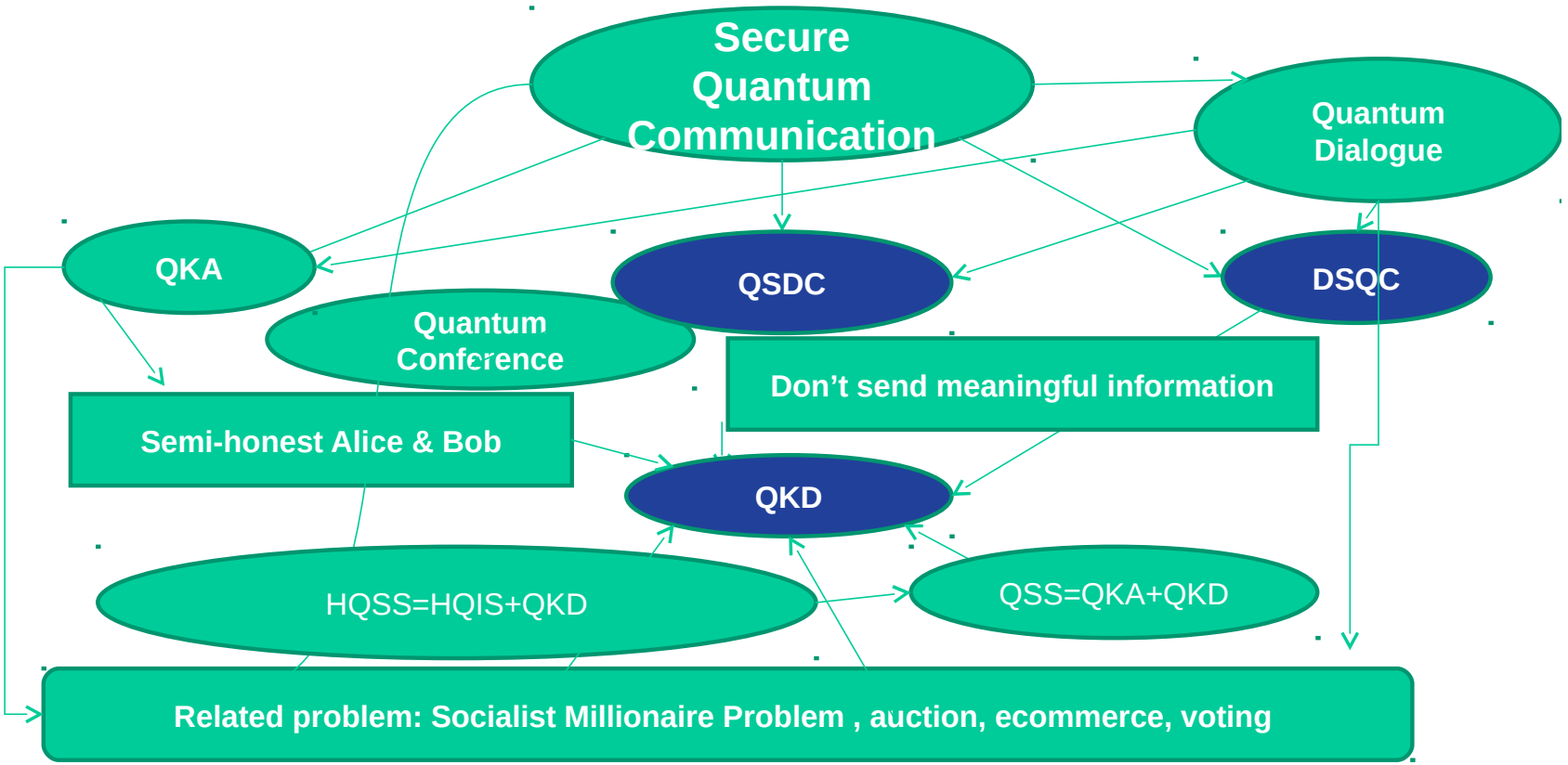
Secure computation and hierarchy of cryptographic primitives



Secure computation and hierarchy of cryptographic primitives

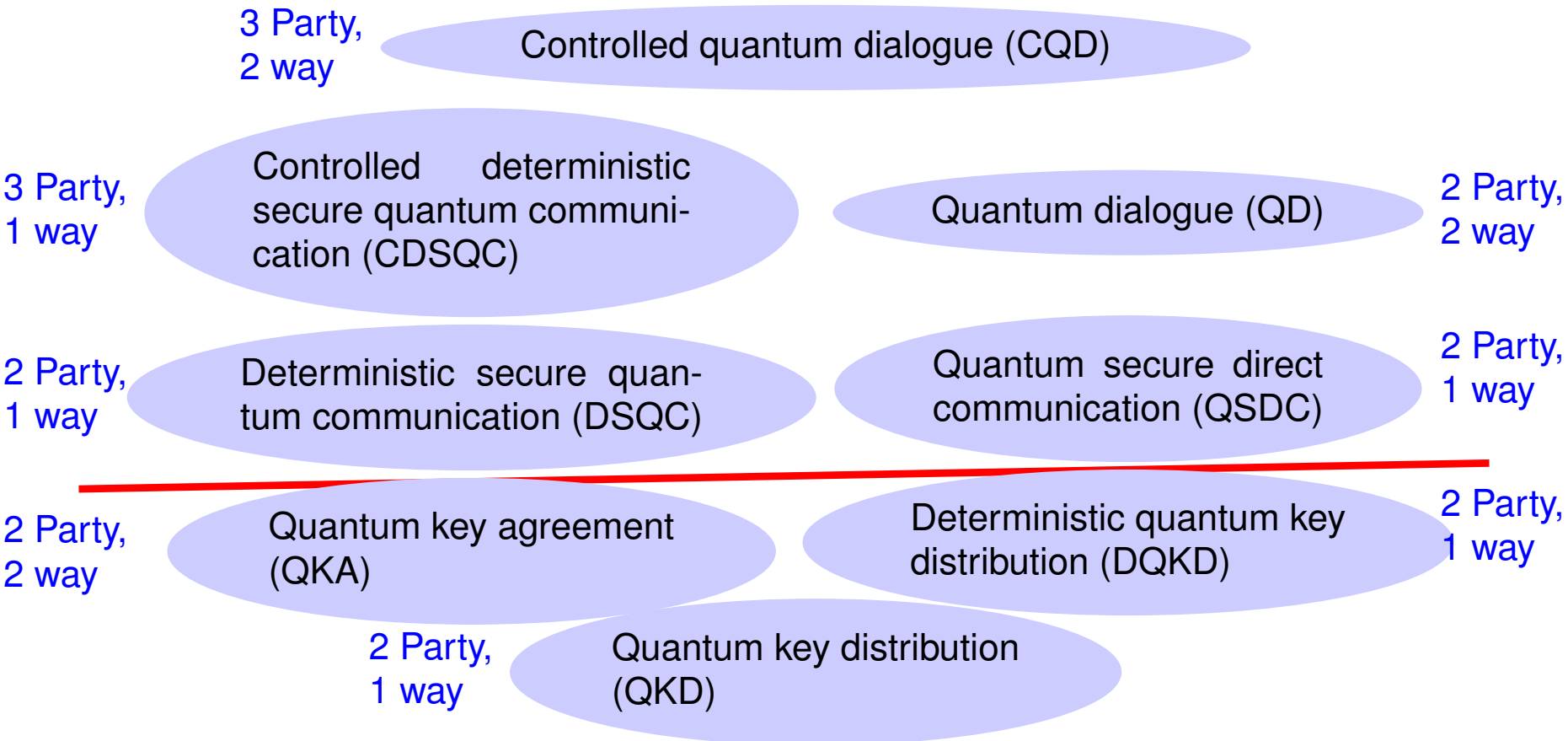


Quantum cryptography



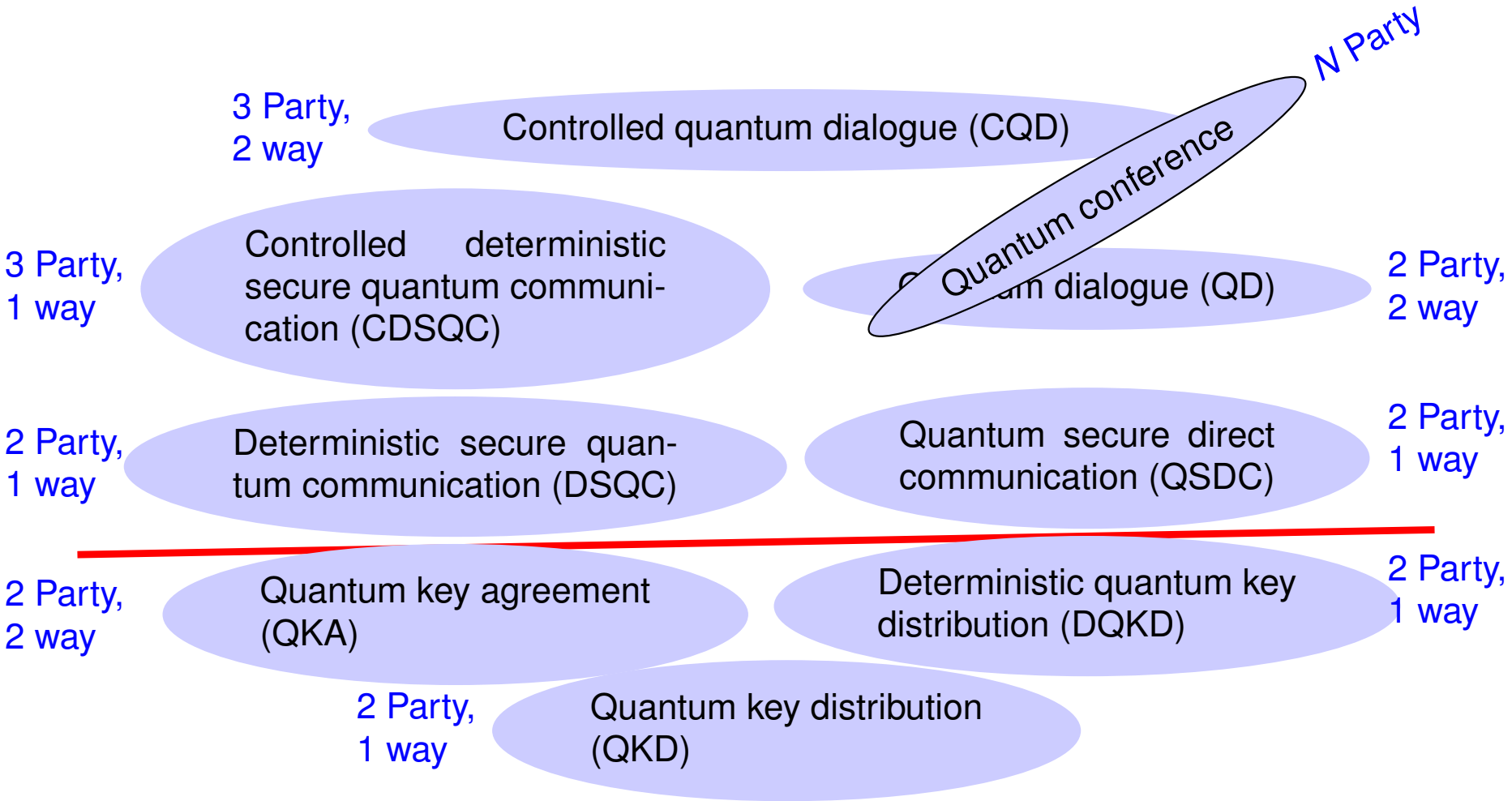
Other relevant problems: HQSS, HDQSS, CQD, C-DSQC, Crypto-Switch, etc.

Hierarchy of quantum cryptography tasks



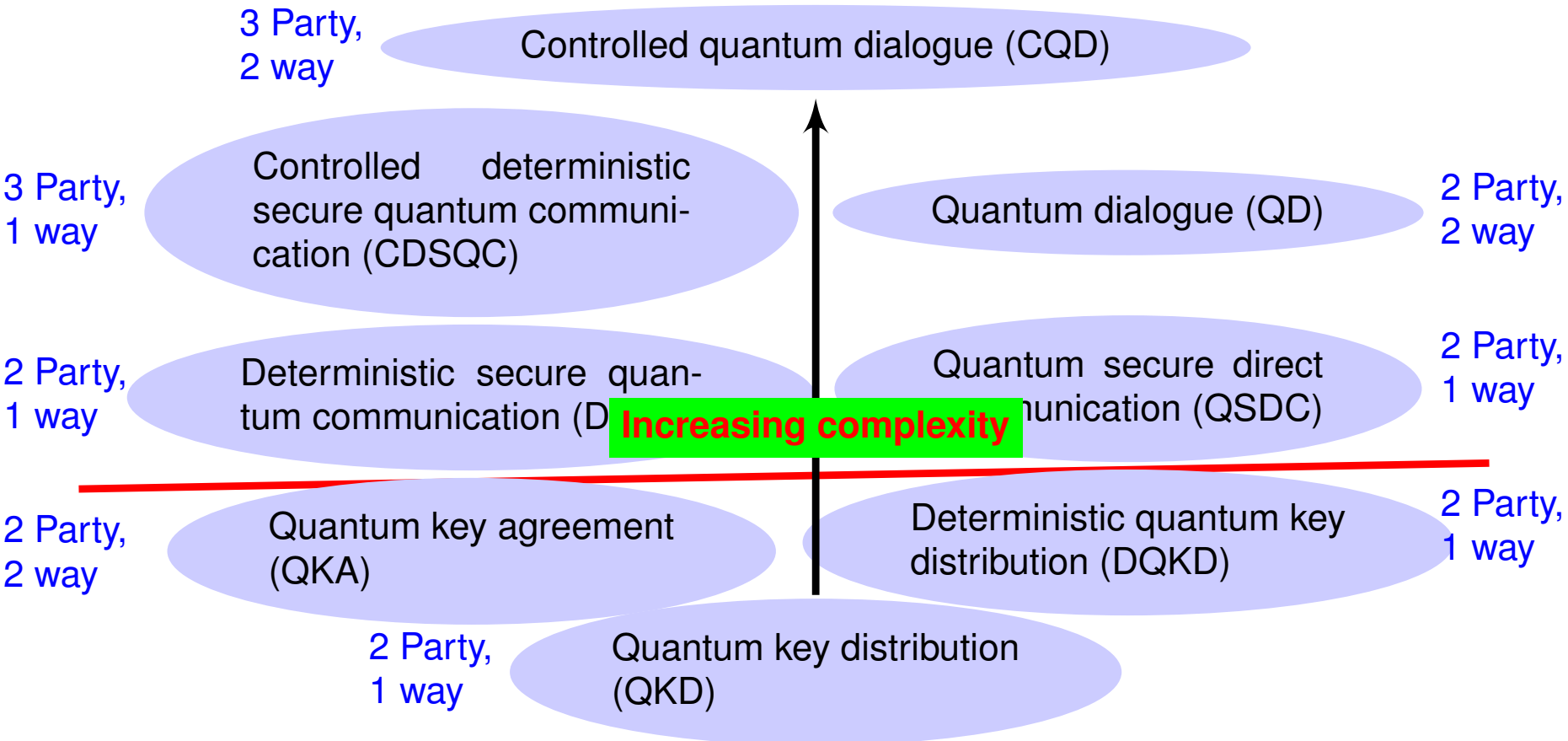
***K. Thapliyal**, A. Pathak, and S. Banerjee, Quantum cryptography over non-Markovian channels, Quantum Inf. Process. 16, 115 (2017).*

Hierarchy of quantum cryptography tasks



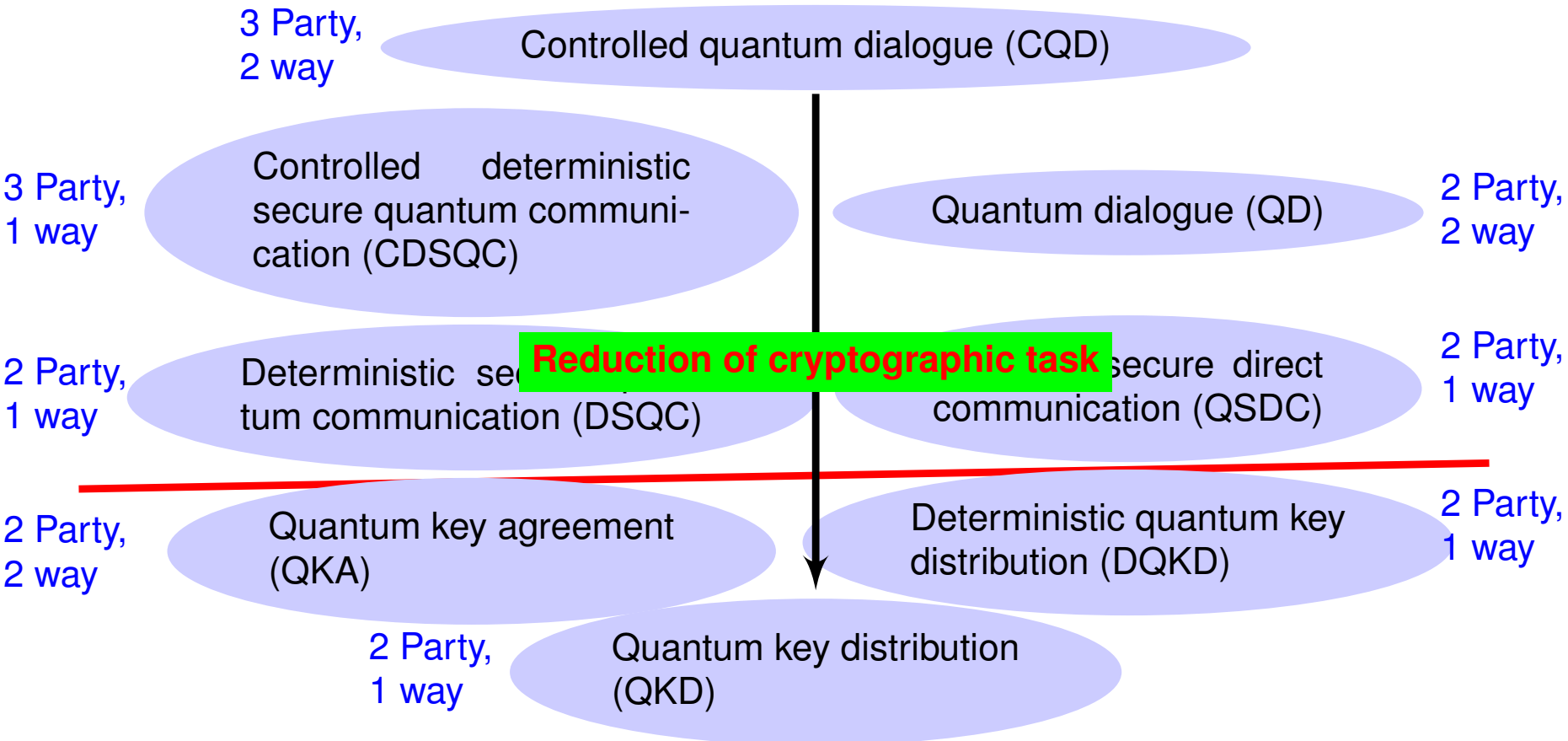
***K. Thapliyal**, A. Pathak, and S. Banerjee, Quantum cryptography over non-Markovian channels, Quantum Inf. Process. 16, 115 (2017).*

Hierarchy of quantum cryptography tasks



***K. Thapliyal**, A. Pathak, and S. Banerjee, Quantum cryptography over non-Markovian channels, Quantum Inf. Process. 16, 115 (2017).*

Hierarchy of quantum cryptography tasks

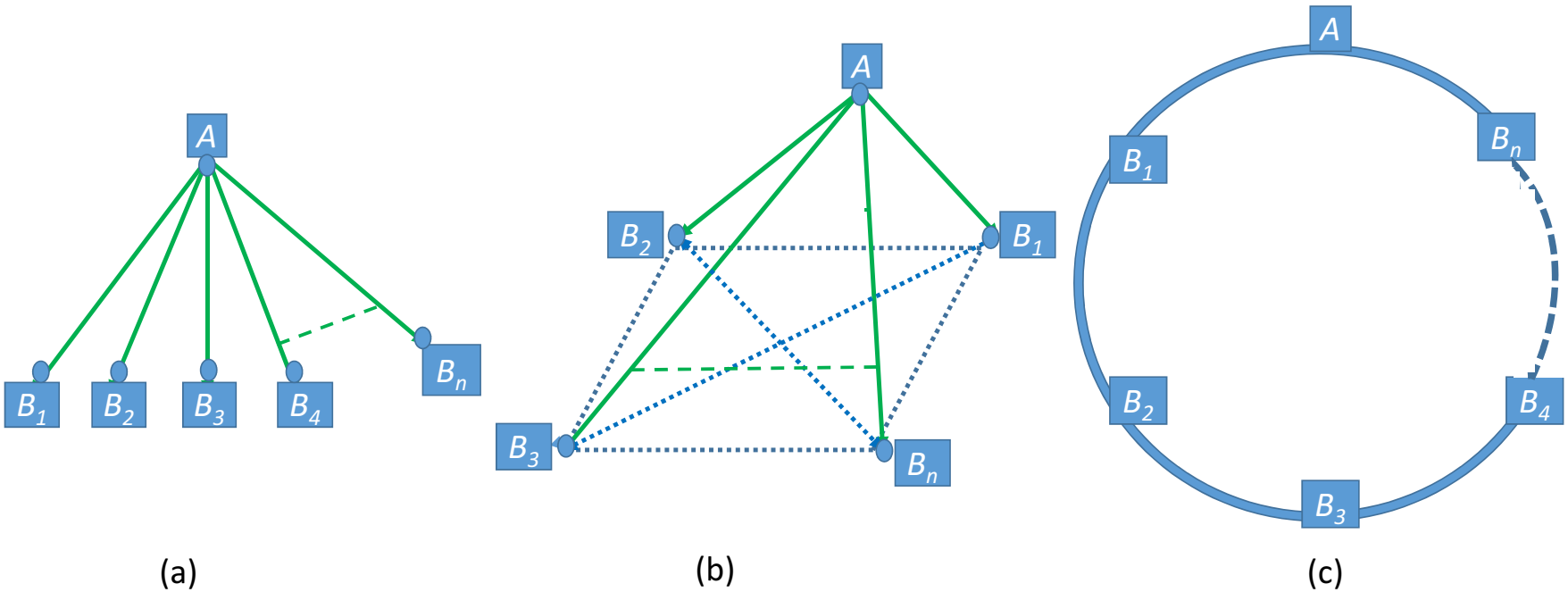


***K. Thapliyal**, A. Pathak, and S. Banerjee, Quantum cryptography over non-Markovian channels, Quantum Inf. Process. 16, 115 (2017).*

Outline

Sealed bid quantum auction

Task: $f(x_1, x_2, x_3, \ldots, x_n) = \max(x_1, x_2, x_3, \ldots, x_n)$

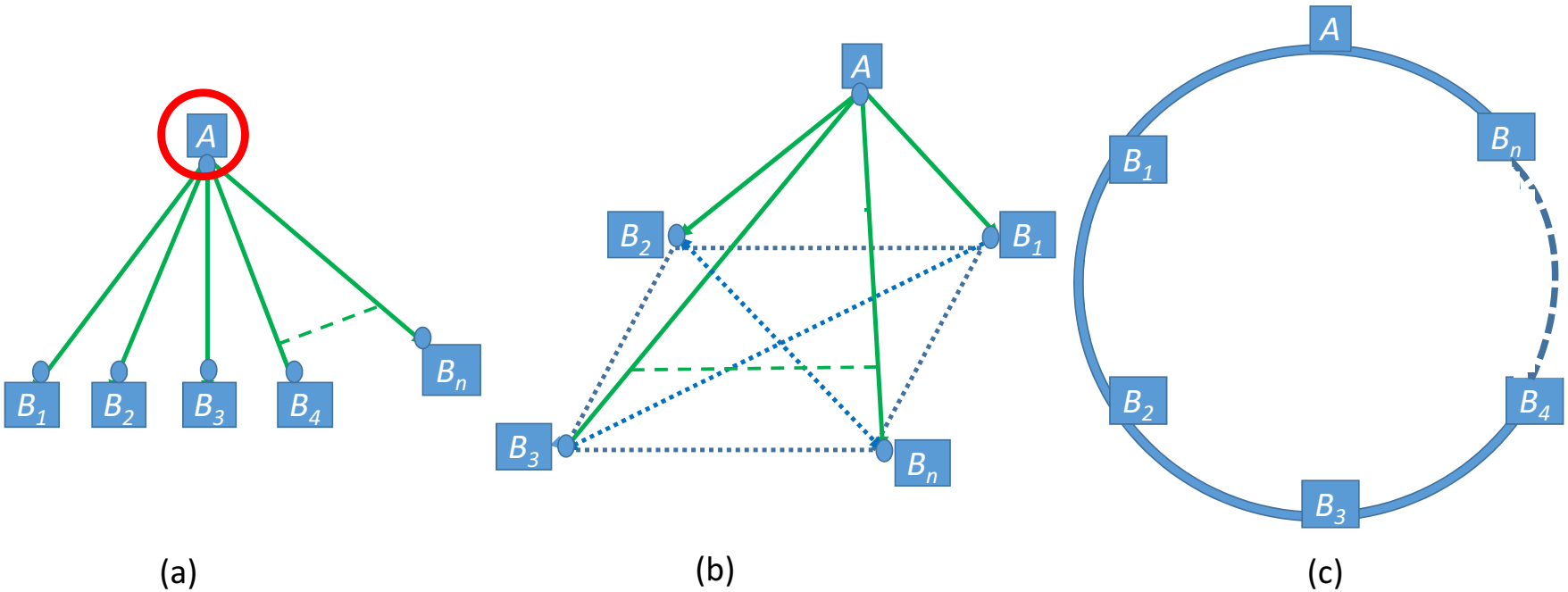


A: Auctioneer; **B:** Bidder

*R. D. Sharma, **K. Thapliyal**, and A. Pathak, Quantum sealed-bid auction using a modified scheme for multiparty circular quantum key agreement, Quantum Inf. Process. 16, 169 (2017).*

Sealed bid quantum auction

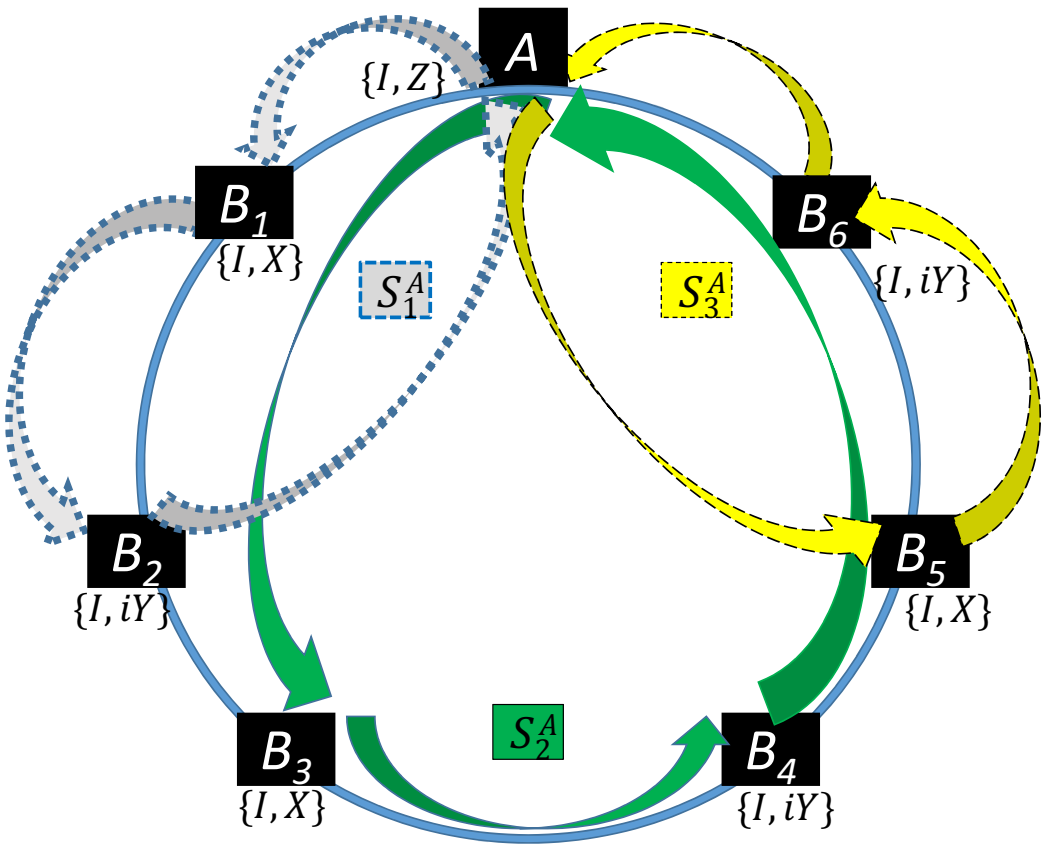
Task: $f(x_1, x_2, x_3, \ldots, x_n) = \max(x_1, x_2, x_3, \ldots, x_n)$



A: Auctioneer; **B:** Bidder

*R. D. Sharma, **K. Thapliyal**, and A. Pathak, Quantum sealed-bid auction using a modified scheme for multiparty circular quantum key agreement, Quantum Inf. Process. 16, 169 (2017).*

Sealed bid quantum auction



Salient features of our scheme:

1. A complete-graph structure is transformed to a circular structure and subsequently that to sub-circles.
2. With an increase in the number of sub-circles, the size of the entangled state required reduces whereas the security against collusion attack increases.
3. This trade-off lessen the requirement of multipartite entanglement, hard to prepare and maintain, leads to better security, and scalability.
4. The present scheme can be performed without an auctioneer.

*R. D. Sharma, **K. Thapliyal**, and A. Pathak, Quantum Inf. Process. 16, 169 (2017).*

Quantum private comparision

Task: $f(x_1, x_2) = \begin{cases} 1 \text{ if } x_1 = x_2 \\ 0 \text{ if } x_1 \neq x_2 \end{cases}$

TP

Millionaire 1

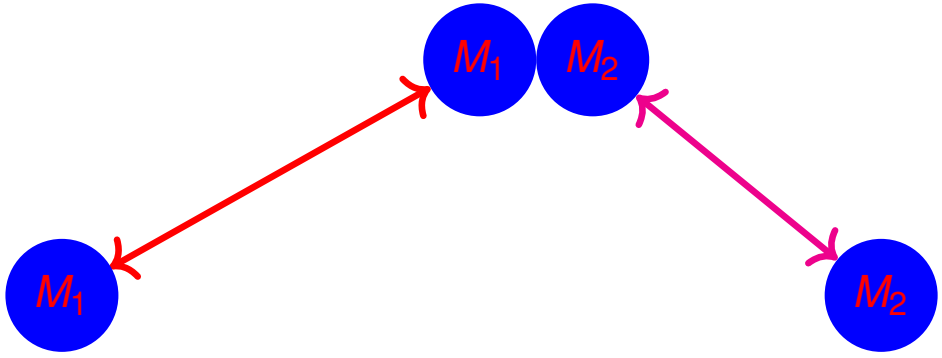
Millionaire 2

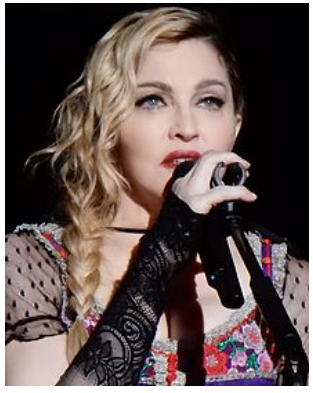
***K. Thapliyal**, R. D. Sharma, and A. Pathak, Int. J. Quantum Inf. 16, 1850047 (2018).*

Quantum private comparision

Task: $f(x_1, x_2) = \begin{cases} 1 \text{ if } x_1 = x_2 \\ 0 \text{ if } x_1 \neq x_2 \end{cases}$

TP





Millionaire 1

Millionaire 2

***K. Thapliyal**, R. D. Sharma, and A. Pathak, Int. J. Quantum Inf. 16, 1850047 (2018).*

Quantum voting

Task: $f(x_1, x_2, x_3, \ldots, x_n) = \sum_i x_i \; \forall x_i : \left\{ \begin{array}{c} x_i = 0 \text{ for “no”} \\ x_i = 1 \text{ for “yes”} \end{array} \right\}$

Voter

K. Thapliyal, *R. D. Sharma, A. Pathak, Int. J. Quantum Inf. 15, 1750007 (2017).*

Quantum voting

Task: $f(x_1, x_2, x_3, \ldots, x_n) = \sum_i x_i \; \forall x_i : \left\{ \begin{array}{c} x_i = 0 \text{ for “no”} \\ x_i = 1 \text{ for “yes”} \end{array} \right\}$

Tallyman

Voter

K. Thapliyal, *R. D. Sharma, A. Pathak, Int. J. Quantum Inf. 15, 1750007 (2017).*

Quantum voting

Task: $f(x_1, x_2, x_3, \ldots, x_n) = \sum_i x_i \; \forall x_i : \left\{ \begin{array}{l} x_i = 0 \text{ for “no”} \\ x_i = 1 \text{ for “yes”} \end{array} \right\}$

Controller

Tallyman

Voter

***K. Thapliyal**, R. D. Sharma, A. Pathak, Int. J. Quantum Inf. 15, 1750007 (2017).*

Quantum voting

Task: $f(x_1, x_2, x_3, \ldots, x_n) = \sum_i x_i \; \forall x_i : \left\{ \begin{array}{l} x_i = 0 \text{ for "no"} \\ x_i = 1 \text{ for "yes"} \end{array} \right\}$

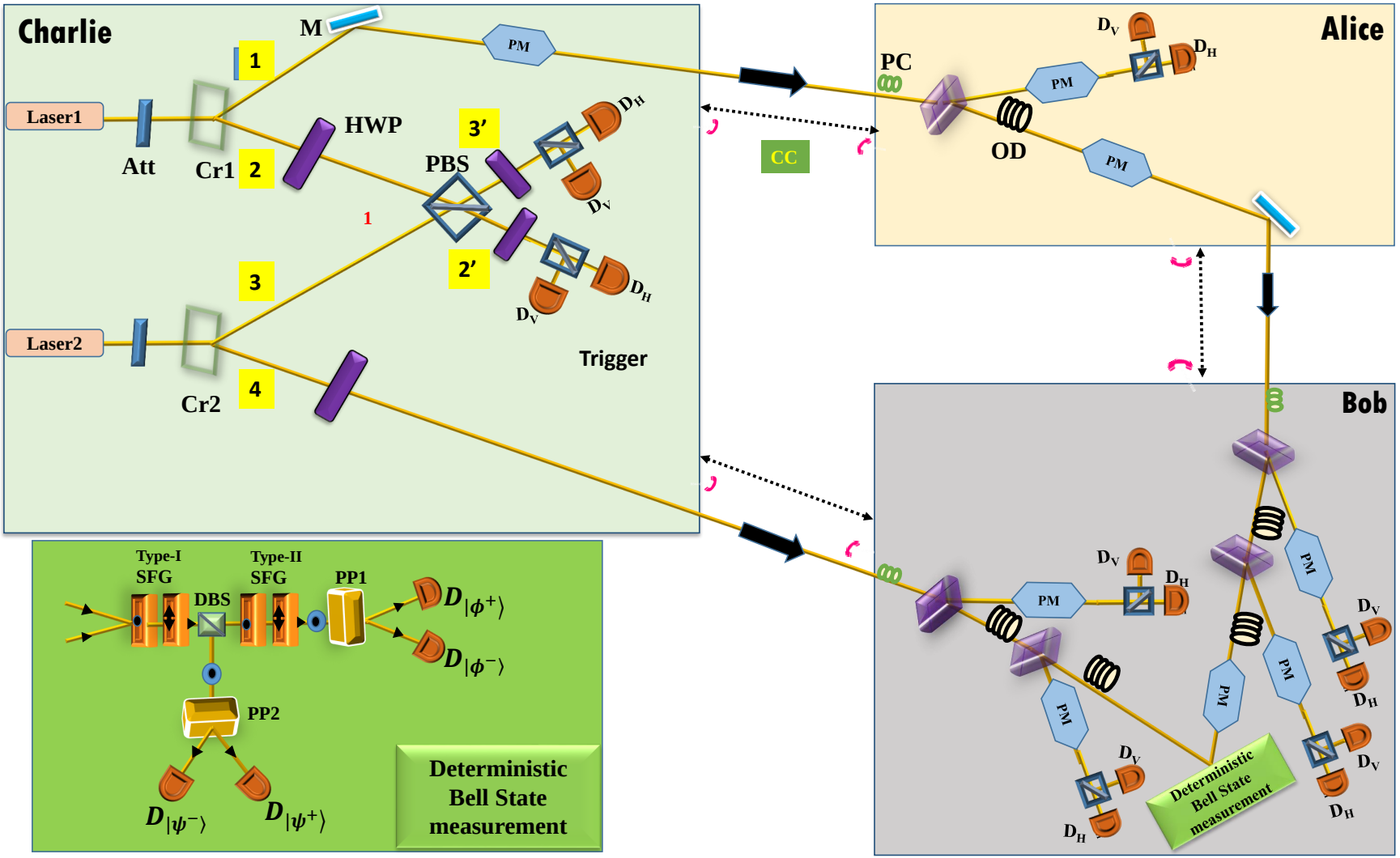
Controller

Tallyman

Voter

***K. Thapliyal**, R. D. Sharma, A. Pathak, Int. J. Quantum Inf. 15, 1750007 (2017).*

Optical design for controlled quantum dialogue



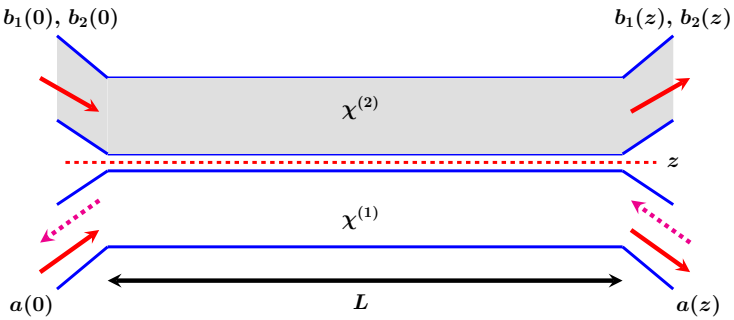
Activities in the field of quantum optics

Optical cavity PRA 97, 063840 (2018) & arXiv: 1708.03967 & Light-semiconductor arXiv:1811.09849

Quantum Zeno effect PRA 93, 022107 (2016) & Parity-Time symmetry arXiv:1811.05604

BEC systems Phys. A 466, 140 (2017) & arXiv: 1708.03967

Spin states Ann. Phys. 362, 261 (2015) & Tomograms Ann. Phys. 366, 148 (2016)



Nonlinear optical couplers PRA 90, 013808 (2014) & PLA 378, 3431 (2014)

Optomechanical system arXiv: 1708.03967 & Coherence arXiv:1811.05599

Engineered quantum states PLA 381, 3178 (2017) & arXiv:1808.01458

Raman and hyper-Raman processes arXiv:1710.04456

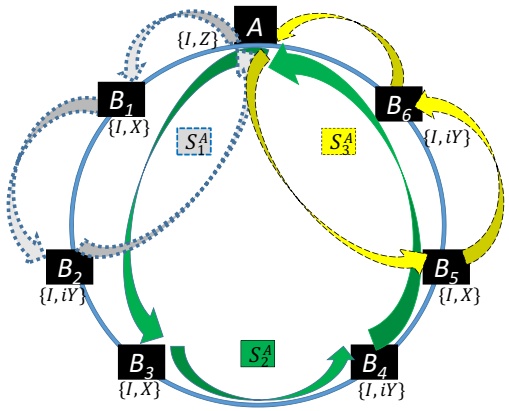
Activities in the field of quantum communication

Teleportation QINP 16, 76 (2017) & QINP 16, 292 (2017) & Controlled teleportation QINP 14, 2599 (2015) & QINP 14, 4601 (2015)

Hierarchical quantum communication QINP 16, 205 (2017)

Direct secure quantum communication QINP 16, 115 (2017) & QINP 17, 229 (2018)

Quantum voting IJQI 15, 1750007 (2017) & Decoy qubits QINP 15, 1703 (2016) & QINP 15, 4681 (2016)



Quantum key distribution arxiv:1609.07473v1 (2016) & Quantum conference QINP 17, 161 (2018)

Controlled direct secure quantum communication QINP 16, 115 (2017) & Semi-quantum QINP 16, 295 (2017) & IJQI 16, 1850047 (2018)

Quantum sealed bid auction QINP 16, 169 (2017) & Asymmetric quantum dialogue QINP 16, 49 (2017)

Quantum e-commerce QINP 16, 295 (2017) & arXiv:1807.08199 & Quantum private comparison IJQI 16, 1850047 (2018)

THANK YOU