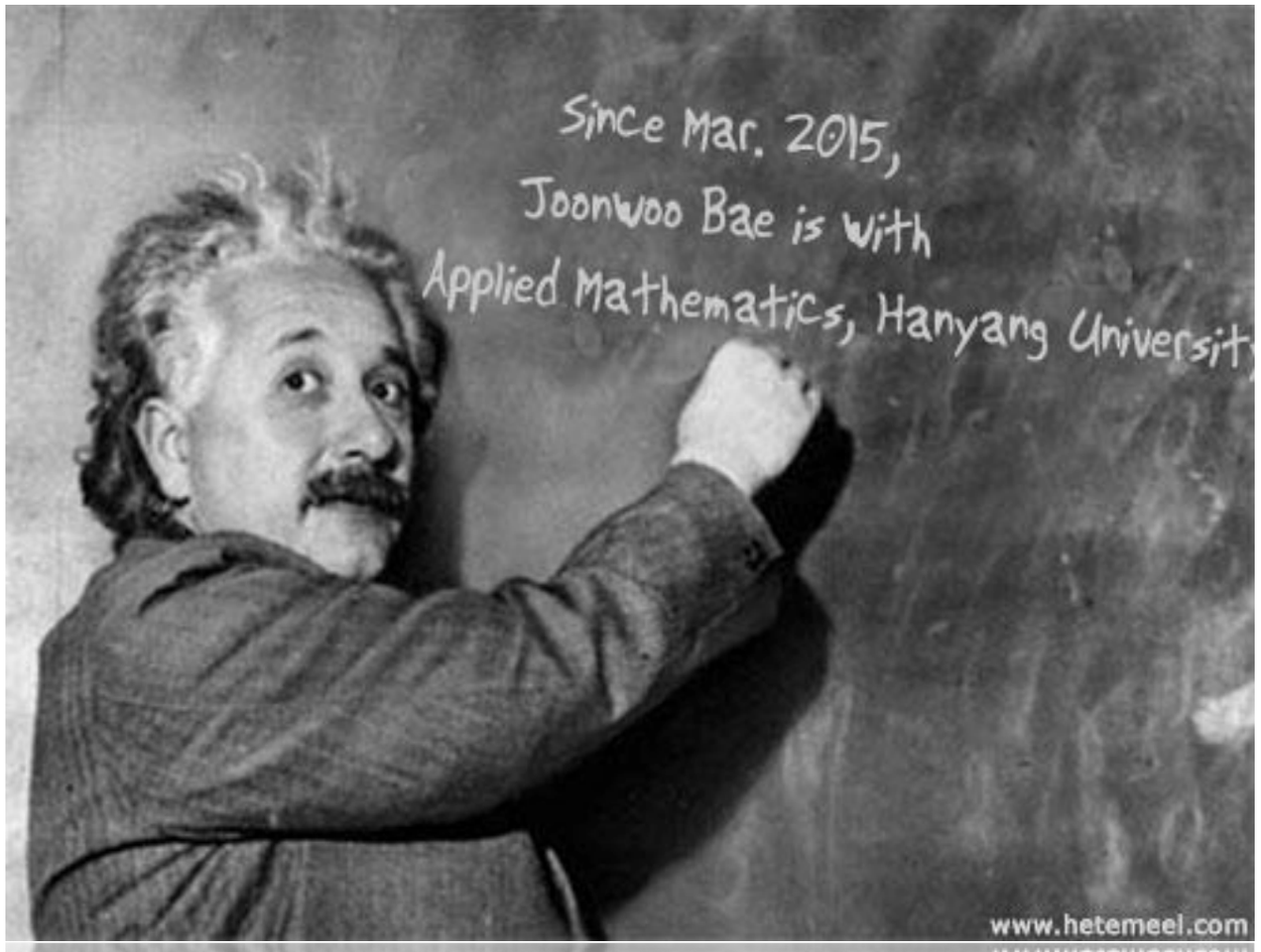
QUANTUM INFORMATION THEORY
applications of the fundamental principles



15-present Dept. of Applied Mathematics, Hanyang Univ. (ERICA)
2016/7 Fellow at Freiburg Institute for Advanced Study (FRIAS)

'14-'15 Freiburg Institute for Advanced Studies (FRIAS), Germany
Junior Fellow, PI at FRIAS, and EU Marie-Curie Fellow (co-fund)

'11-'14 Superpositions of
Centre for Quantum Technologies (CQT), Singapore and
ICFO-Institute of Photonic Sciences, Barcelona

'07-'11 Korea Institute for Advanced Study (KIAS)
PI in GEnKO project, of Korea and Germany

'03-'07 Univ. de Barcelona and ICFO
(the field of specialisation: Quantum Information Theory)

Thesis title: Entanglement and Quantum Cryptography
i) security analysis of quantum cryptography, ii)open problems

'01-'03 Hanyang Univ. (Phys.)

98-'01 Hanyang Univ. (major in Math. with minor in Phys.)

FRIAS
FREIBURG INSTITUTE FOR ADVANCED STUDIES

HANYANG UNIVERSITY 한양 1939

KIST
Korea Institute of Science and Technology

IITP
Institute for Information & communications Technology Promotion

INTERNATIONAL BUSINESS TIMES
MONDAY, MAY 11, 2015 AS OF 3:35 AM EDT

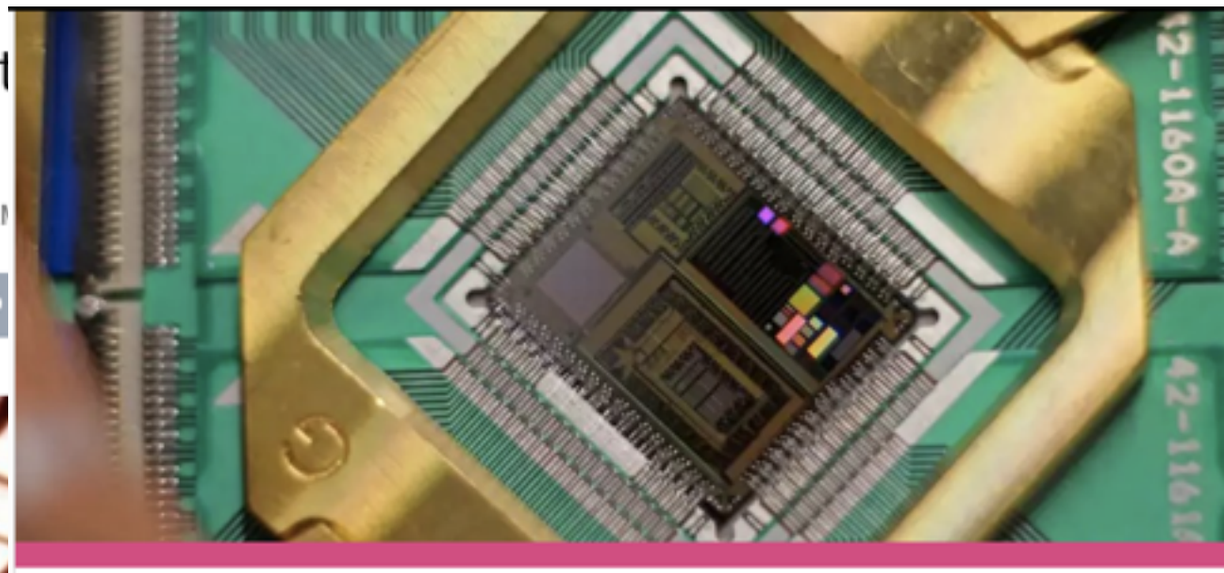
TECHNOLOGY COMPUTERS

Google Announces It Is Developing New Super-Fast Quantum Computing Chip With UC Santa Barbara

By Harichandan Arakali @bangalorejourno h.arakali@ibtimes.com on September 03 2014 3:18 AM

Quantum Computing

Creating a new generation of computin

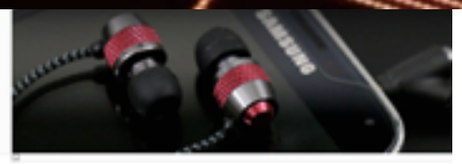


Google's quantum computer just accurately simulated a molecule for the first time

It's a quantum world, we're just living in it.

DAVID NIELD 22 JUL 2016

› '일본 침몰' 세계 TV시장 삼성·LG 지배력↑
› 만원짜리 초소형 컴퓨터 등장!…사양 봤더니
› 갤S6 엣지의 숨은 주역…中서 '러브콜' 까지
› 日서 금융IT 수입한 한국, 이젠 10년 앞섰다!



 발행일 2014.12.10

폰트 +

KT도 양자암호통신…SKT와 '퀀텀 경쟁'

[단독] 10만원대 프리미엄 이어폰도 2만원대로

KT가 양자암호통신 기술 파악에 착수한다.

KT에 앞서 양자암호통신 기술 개발에 돌입한 SK텔레콤과의 경쟁도 본격화될 전망이다.

SK텔레콤, 차세대 통신보안기술 '양자암호통신' 시제품 국내 최초로 선보여 - T뉴스

뉴스
2014/10/20 09:42

T뉴스

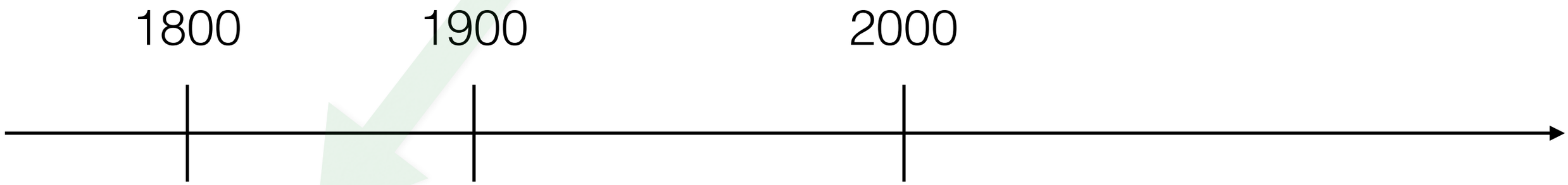
SK텔레콤,
차세대 통신보안기술
'양자암호통신' 시제품
국내 최초로 선보여

Information Technology

Applied Math.

Computation Theory
(*a la* Turing)

Communication Theory
(*a la* Shannon)



Physics

Electromagnetism

Information Technology

Quantum IT?

Applied Math.

Computation Theory
(*a la* Turing)

Quantum Computation

Communication Theory
(*a la* Shannon)

Quantum Communication

1800 1900 2000

Physics

Electromagnetism

Quantum Theory

Alexander S. Holevo (Shannon Award)

Steklov Mathematical Institute, Russia

A. S. Holevo's scientific interests lie in the foundations of quantum theory, quantum statistics and quantum information theory. In 1973 he obtained an upper bound for amount of classical information which can be extracted from ensemble of quantum states by quantum measurements (this result is known as Holevo's theorem). He also developed the mathematical theory of quantum communication channels, the noncommutative theory of statistical decisions, proved coding theorems in quantum information theory and revealed the structure of quantum Markov semigroups and measurement processes.

Alexander S. Holevo graduated f
Thesis in 1975. Since 1986 A. S.
honors, Alexander Holevo receiv
Russian Academy of Sciences (
and the Claude E. Shannon Awa

Theory of Probability & Its Applications

< Previous Article

Volume 60, Issue 3

Abstract | PDF

Theory Probab. Appl., 60(3), 501–501. (1 page)

The Claude E. Shannon Award

M. V. Khatuntseva

DOI:10.1137/S0040585X97T98779X

Alexander Semenovich Holevo is honored with the 2016 Claude E. Shannon Award for his fundamental contributions to quantum information theory.

Claude E. Shannon Award

From Wikipedia, the free encyclopedia

The **Claude E. Shannon Award** of the IEEE Information Theory Society was instituted to honor consistent and profound contributions to the field of Information Theory. Each Shannon Award winner is expected to present a Shannon Lecture at the following IEEE International Symposium on Information Theory.[1] It is the most prestigious prize in Information Theory, covering technical contributions at the intersection of mathematics, communication engineering, and theoretical computer science.

It is named for Claude E. Shannon, who was also the first recipient.

Recipients [edit]

The following people have received the Claude E. Shannon Award:[2]

- 1972 – Claude E. Shannon
- 1974 – David S. Slepian
- 1976 – Robert M. Fano
- 1977 – Peter Elias
- 1978 – Mark Semenovich Pinsker
- 1979 – Jacob Wolfowitz
- 1981 – W. Wesley Peterson
- 1982 – Irving S. Reed
- 1983 – Robert G. Gallager
- 1985 – Solomon W. Golomb
- 1986 – William Lucas Root
- 1988 – James Massey
- 1990 – Thomas M. Cover
- 1991 – Andrew Viterbi
- 1993 – Elwyn Berlekamp
- 1994 – Aaron D. Wyner
- 1995 – George David Forney
- 1996 – Imre Csiszár
- 1997 – Jacob Ziv
- 1998 – Neil Sloane
- 1999 – Tadao Kasami
- 2000 – Thomas Kailath
- 2001 – Jack Keil Wolf
- 2002 – Toby Berger
- 2003 – Lloyd R. Welch
- 2004 – Robert McEliece
- 2005 – Richard Blahut
- 2006 – Rudolf Ahlswede
- 2007 – Sergio Verdú
- 2008 – Robert M. Gray
- 2009 – Jorma Rissanen
- 2010 – Te Sun Han
- 2011 – Shlomo Shamai (Shitz)
- 2012 – Abbas El Gamal[3]
- 2013 – Katalin Marton[4]
- 2014 – János Körner
- 2015 – Robert Calderbank
- 2016 – Alexander Holevo
- 2017 – David Tse[5]

Take-home message: We're on the way to Quantum Era

Information Technology

Quantum IT?

Applied Math.

Computation Theory
(*a la* Turing)

Quantum Computation

Probability
Information Theory

Communication Theory
(*a la* Shannon)

Quantum Communication

1800 1900 2000

Physics

Electromagnetism

Quantum Theory

Information Flow ~

Motivation

Fundamentals of Quantum Information Theory

Applications

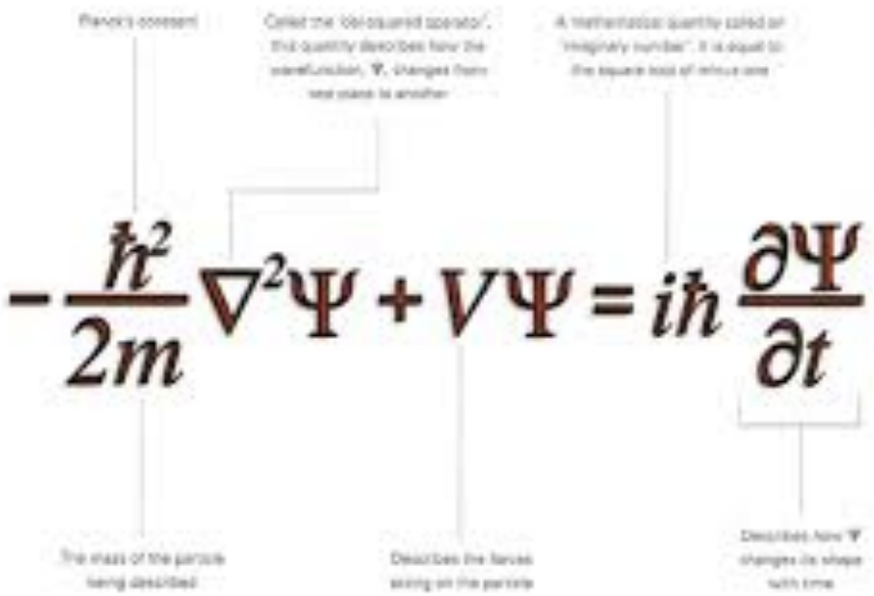
Single, Bi-partite, Tri-partite, …

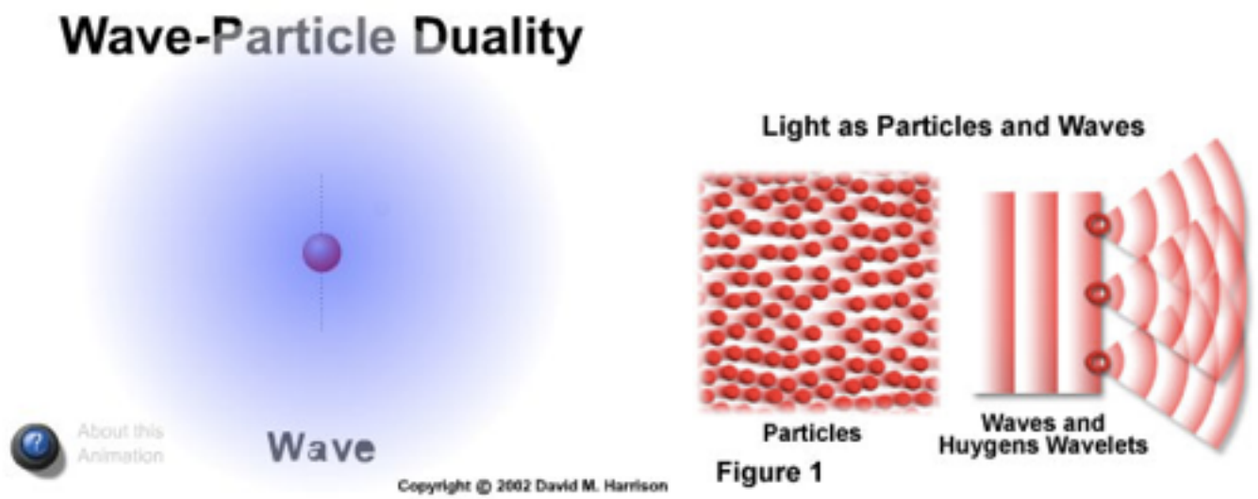
QUANTUM THEORY

in the view of a quantum information theorist

What is Quantum Mechanics?

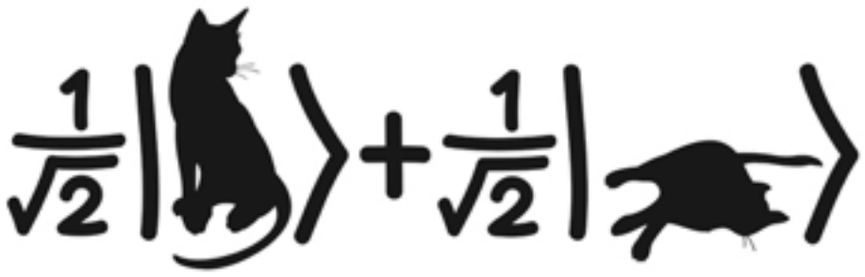
Schrodinger Eq.?

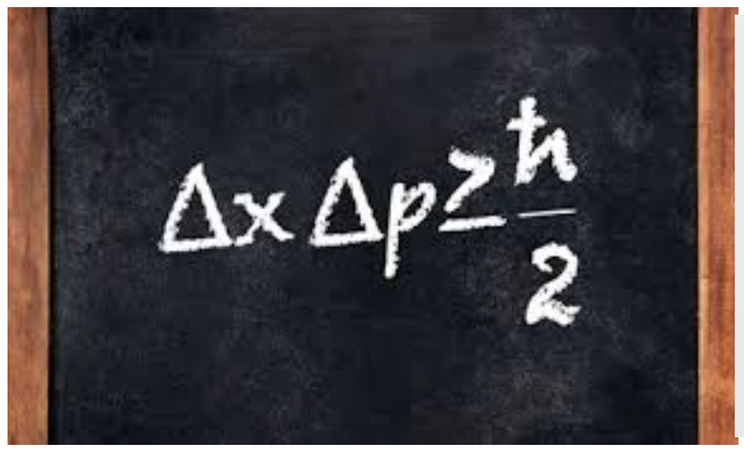


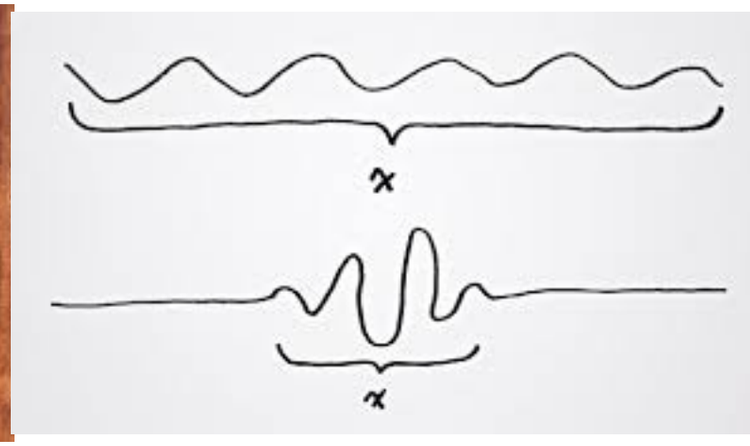


Uncertainty principle?

Superposition principle?
dead or alive







Quantum Theory

Stochastic Process

$\mathrm{C}^* - \mathrm{algebra}$

Gelfand-Naimark-Segal (GNS) construction

$\mathrm{Prob[X|Y]}$

Bounded operators in Hilbert spaces

(Operator algebra)

(Operator space theory)

Information Theory

Representation

Entropies $\mathrm{H(X)},\ \mathrm{I(X:Y)},$ etc.

Matrix algebra

Quantum Theory

Information Theory

Quantum systems, Dynamics, Statistics

Coding $\mathrm{H}(\mathrm{X})$

states: $\rho \in \mathcal{M}_n \quad \mathcal{M}_n := \mathcal{M}_n^{\geq}$ non-negative matrices

Communication $\mathrm{I}(\mathrm{X}:\mathrm{Y})$

measurement: $M \in \mathcal{M}_n \quad M \geq 0$

Estimation, etc. $\mathcal{F}(\mathcal{N}),\ \mathcal{L}(\mathcal{N}|\mathcal{D})$

probabilities $p(M|\rho) = \mathrm{tr}[M\rho]$

*Martingale, Makovianity… etc.
*Convex Optimisation
(Semidefinite Programming)
*Compressive sensing (wavelet)

Gleason's theorem: Born rule

Matrix algebra

Prob[X|Y]

Quantum Information Theory

Quantum Information Theory ρ_{AB}	vs.	Information Theory p_{AB}
Qubit		Bit
Entangled bit		Secret bit
Quantum teleportation		One-time pad
Entanglement distillation		Secret key distillation
Separable states (LOCC)		Separable correlations (Public Communication)
Bound entanglement		Bound information
Quantum Shannon Theory		Shannon Theory

D Collins and S Popescu PRA 65 032321 (2002)

Unit of quantum information processing: QUantum BIT (QUBIT)

Qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

E_1 ——— $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

E_0 ——— $|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

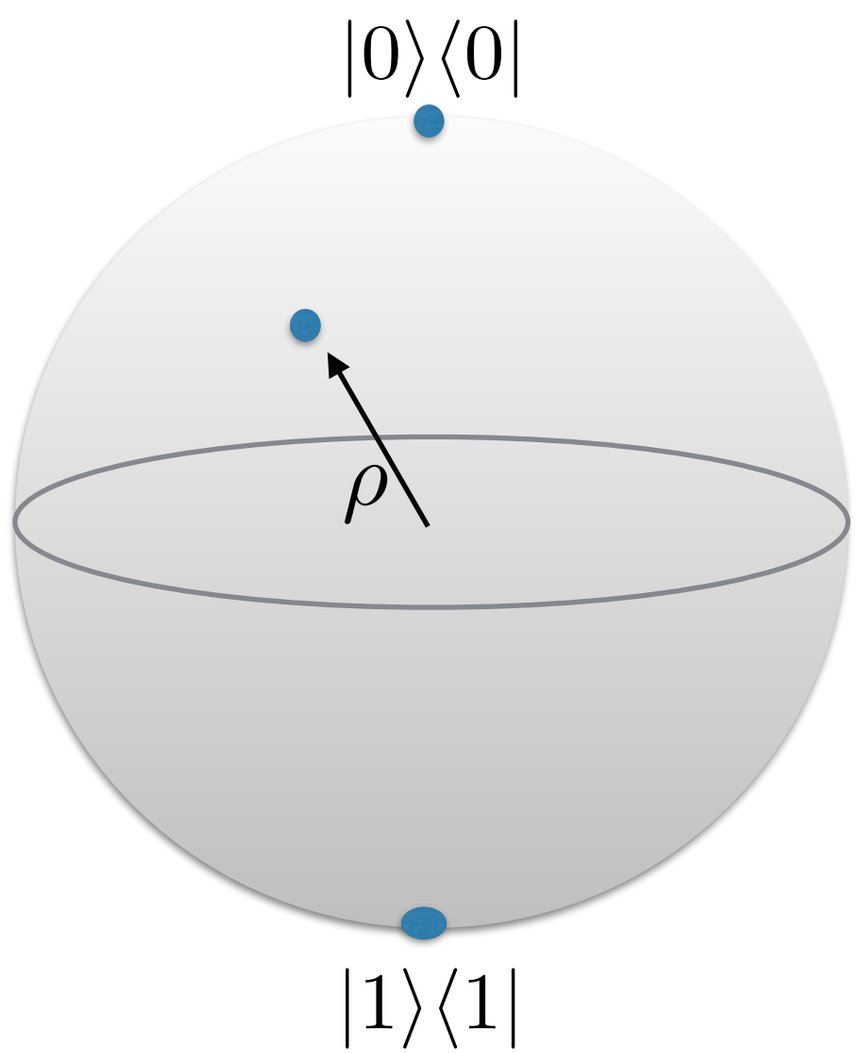
states: $\rho \in \mathcal{M}_n \qquad \rho \geq 0$

Qubit state : Any two-level system

$$\rho = \frac{1}{2}\begin{pmatrix} 1+\cos\theta & e^{-i\phi}\sin\theta \\ e^{i\phi}\sin\theta & 1-\cos\theta \end{pmatrix}$$

Bit

Information Unit: Bit $\quad 0,\ 1$

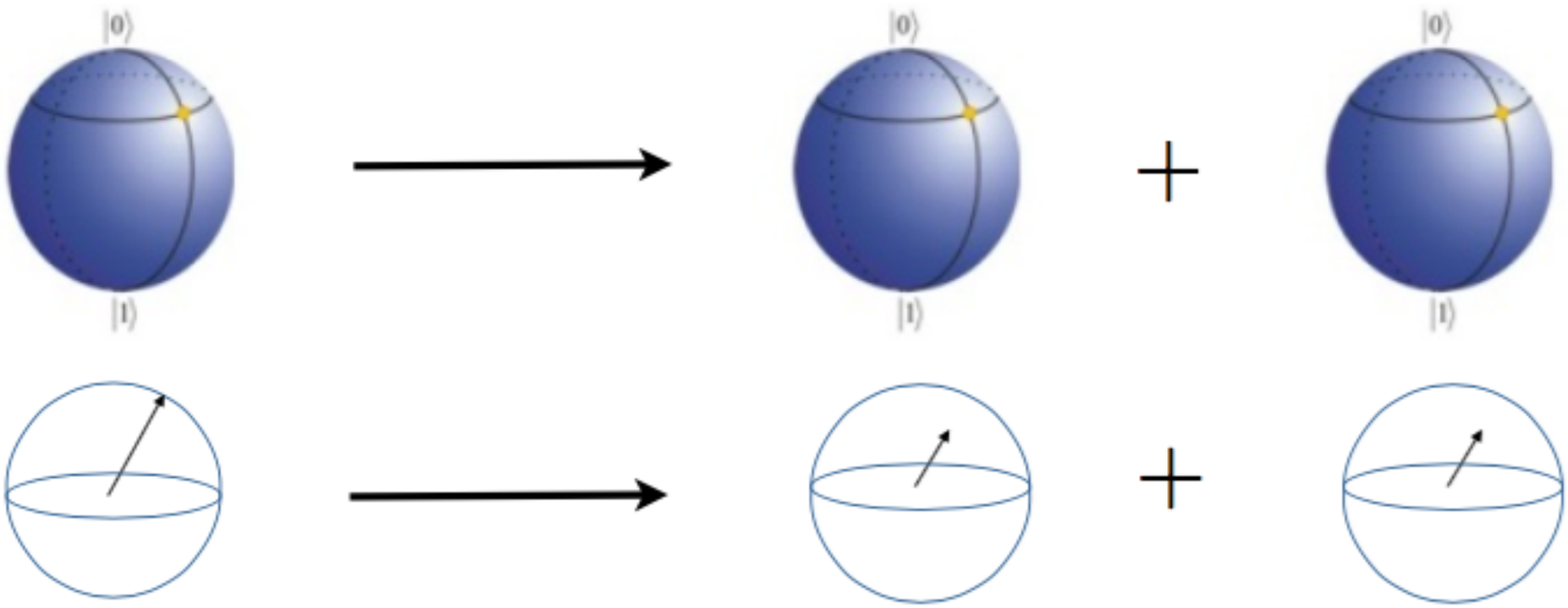


Story One: Information of Single Quantum Systems

Single quantum states cannot be copied

Quantum cloning

$1 \to 2$



$|\psi\rangle$ $\rho_\psi \approx |\psi\rangle$

Optimizing quantum operations

$$F_Q = \langle\psi|\rho_\psi^{(Q)}|\psi\rangle = \frac{5}{6}$$

Trivial strategy from optimal measurement and state-preparation
(State Estimation)

$$F_M = \langle\psi|\rho_\psi^{(M)}|\psi\rangle = \frac{2}{3}$$

$$F_Q > F_M$$

THE CARELESS USE OF LANGUAGE IN QUANTUM INFORMATION

K. WIESNER

School of Mathematics
University of Bristol, Bristol, BS8 1TW, U.K.

An imperative aspect of modern science is that scientific institutions act for the benefit of a common scientific enterprise, rather than for the personal gain of individuals within them. This implies that science should not perpetuate existing or historical unequal social orders. Some scientific terminology, though, gives a very different impression. I will give two examples of terminology invented recently for the field of quantum information which use language associated with subordination, slavery, and racial segregation.

My first example is the term 'ancilla qubit'. In a quantum computational algorithm the relevant information is stored in quantum states which, in analogy to 'bits' in classical

My second example of the use of language in quantum information is 'quantum supremacy'. It is the name of a subfield in quantum information which has just begun to emerge. This subfield is concerned with the search for tools to computationally simulate quantum systems that are too hard to be simulated with classical computational tools. The hope is to gain insights into the behaviour of highly correlated quantum matter beyond what can be achieved with classical computers. The English word 'supremacy' denotes the quality or

Learning from the history

1970

1980

A. Holevo, Problems of Information Transmission (1974)
H. Yuen, R. Kenney, and M. Lax, IEEE Trans. Inf. Theory (1975)
C. Helstrom, Quantum Detection and Estimation Theory (1976)

Quantum Signal Processing
(Quantum State Discrimination/Estimation)

W. K. Wootters and W. Zurek, “A single quantum cannot be cloned”
Nature 229 802 (1982)

Quantum Cryptography

C. H. Bennett and G. Brassard, “Quantum Cryptography”, Bangalore (1984)

No-Cloning Theorem

PHYSICAL REVIEW A VOLUME 54, NUMBER 3 SEPTEMBER 1996

Quantum copying: Beyond the no-cloning theorem

V. Bužek[1,2] and M. Hillery[1]
[1]*Department of Physics and Astronomy, Hunter College of the City University of*
695 Park Avenue, New York, New York 10021
[2]*Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 842 28 Bratisl*
(Received 5 February 1996)

We analyze the possibility of copying (that is, cloning) arbitrary states of a quantum-m system. We show that there exists a "universal quantum-copying machine" (i.e., transfor proximately copies quantum-mechanical states such that the quality of its output does not de We also examine a machine which combines a unitary transformation and a selective measu good copies of states in the neighborhood of a particular state. We discuss the problem of n output states. [S1050-2947(96)08408-9]

PACS number(s): 03.65.Bz

JOURNAL OF MATHEMATICAL PHYSICS VOLUME 40, NUMBER 7 JULY 199

Optimal cloning of pure states, testing single clones

M. Keyl[a)] and R. F. Werner[b)]
Institut für Mathematische Physik, TU Braunschweig, Mendelssohnstraße 3,
38106 Braunschweig, Germany

(Received 4 August 1998; accepted for publication 7 April 1999)

We consider quantum devices for turning a finite number N of d-level quantum systems in the same unknown pure state σ into $M>N$ systems of the same kind, in an approximation of the M-fold tensor product of the state σ. In a previous paper it was shown that this problem has a unique optimal solution, when the quality of the output is judged by arbitrary measurements, involving also the correlations between the clones. We show in this paper, that if the quality judgment is based solely on measurements of single output clones, there is again a unique optimal cloning device, which coincides with the one found previously. © *1999 American Institute of Physics.* [S0022-2488(99)03707-X]

VOLUME 79, NUMBER 11 PHYSICAL REVIEW LETTERS 15 SEPTEMBER 1997

Optimal Quantum Cloning Machines

N. Gisin[1] and S. Massar[2]
[1]*Group of Applied Physics, University of Geneva, 1211 Geneva, Switzerland*
[2]*Raymond and Beverly Sackler Faculty of Exact Sciences, School of Physics and Astronomy, Tel-Aviv University,*
Tel-Aviv 69978, Israel
(Receiv

We present quantum cloning machines that t
and we prove that the fidelity (quality) of these
measurement is discussed in detail. When the
each clone tends towards the optimal fidelity th
More generally, quantum cloning machines are
classical information. [S0031-9007(97)0391

PACS numbers: 89.70.+c, 03.65.–w

VOLUME 81, NUMBER 12 PHYSICAL REVIEW LETTERS 21 SEPTEMBER 1998

Optimal Universal Quantum Cloning and State Estimation

Dagmar Bruss,[1] Artur Ekert,[2] and Chiara Macchiavello[3,1]
[1]*ISI, Villa Gualino, Viale Settimio Severo 65, 10133 Torino, Italy*
[2]*Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, United Kingdom*
[3]*Dipartimento di Fisica "A. Volta" and INFM, Via Bassi 6, 27100 Pavia, Italy*
(Received 1 December 1997)

We derive a tight upper bound for the fidelity of a universal $N \rightarrow M$ qubit cloner, valid for any $M \geq N$, where the output of the cloner is required to be supported on the symmetric subspace. Our proof is based on the concatenation of two cloners and the connection between quantum cloning and quantum state estimation. We generalize the operation of a quantum cloner to mixed and/or entangled input qubits described by a density matrix supported on the symmetric subspace of the constituent qubits. We also extend the validity of optimal state estimation methods to inputs of this kind. [S0031-9007(98)07141-5]

m-to-n quantum cloning for qubit states

i) Universal cloning: Gisin and Massar 1997
Werner 1999
ii) Phase-covariant cloning: Bruss et al. (2000)

$$m \to n$$

quantum cloning

$$F_Q = \langle\psi|\rho^{(Q)}|\psi\rangle = \frac{nm+n+m}{n(m+2)} \xrightarrow[n\to\infty]{} \frac{m+1}{m+2}$$

$\rho^{(Q)}$

$|\psi\rangle^{\otimes m}$ $\quad F_Q > F_M$

$$F_M = \langle\psi|\rho^{(M)}|\psi\rangle = \frac{m+1}{m+2}$$

$$\boxed{F_Q^{\infty} = F_M} \; ?$$

$\rho^{(M)}$

i) Universal qubit cloning:
Bruss, Ekert, and Macchiavello (1998)
ii) Universal qudit cloning:
Keyl and Werner (1999)
iii) General case:
Bae and Acin (2007);
Chiribella and D'Ariano (2007)

State estimation

Massar and Popescu 1995

Optimal Cloning of Quantum States

1980

W. K. Wootters and W. Zurek "No-Cloning Theorem" (1982)

1990

One-to-Two Universal Symmetric Qubit Cloning (V Buzek and M Hillery 1996)
General Universal Quantum Cloning (N Gisin and S Massar 1997)
Optimal Cloning (R. F. Werner 1999)
Optimal Qubit Cloning and State Estimation (D. Bruss, C. Macchiavello, A Ekert 1998,2000)

2000

Application to Quantum Key Distribution, Review on "Quantum Key Distribution"
E.g. Quantum Cryptography RMP (N Gisin, G Ribordy, W Tittel, and H. Zbinden 2002)
The Security of Practical QKD, RMP (V. Scarani et al. 2009)
Review on Quantum Cloning, (V Scarani, S. Iblisdir, N Gisin and A Acin, RMP 2005)
Asymptotic quantum cloning is state estimation (J Bae and A Acin 2006)

What's OQP – Open Quantum Problems?

Solved Quantum Problems

Show 50

Nr	Title					
10	Additivity of classical capacity and related problems	A.S. Holevo	2003/01/31	2004/11/11	M. Hastings	Quantum communication
18	Qubit bi-negativity	K.G.H. Vollbrecht	2003/02/10	2005/04/22	S. Ishizaka	Entanglement theory
19	Stronger Bell Inequalities for Werner states?	N. Gisin	2003/06/20	2008/05/02	T. Vértesi	Quantum foundations
21	Bell violation by tensoring	Y.-C. Liang	2005/02/08	2010/10/25	M. Navascués and T. Vértesi	Quantum foundations
22	Asymptotic cloning is state estimation	M. Keyl	2005/02/08	2006/11/01	J. Bae and A. Acín	Quantum communication
28	Local equivalence of graph states	D. Schlingemann	2005/04/20	2007/09/09	Z. Ji, J. Chen, Z. Wei, M. Ying	Entanglement theory
30	Asymptotic Version of Birkhoff's Theorem	A. Winter	2005/10/06		M.Musat, H.Haagerup	Quantum communication

Asymptotic cloning is state estimation

Cite as: http://qig.itp.uni-hannover.de/qiproblems/22

Previous problem: Bell violation by tensoring

Next problem: SIC POVMs and Zauner's Conjecture

Contents [hide]

Problem

Fix an arbitrary probability measure on the pure states of a d-dimensional quantum system. Let $F(N,M)$ be the optimal single copy fidelity for N-
transformations, averaged with respect to the given probability measure and over all M clones.

On the other hand, let $F(N,\infty)$ be the best mean fidelity achievable by measuring on N input copies of the state, and repreparing a state ac
measured data. The problem is to decide whether one always gets $\lim_{M\to\infty} F(N,M) = F(N,\infty)$.

It is clear that the limit exists, because $F(N,M)$ is non-increasing in M. Moreover, the limit will be larger or equal than the right hand side, becau
with repreaparation is a particular cloning method. A weaker, but still interesting version of the problem is whether the above equation become
limit $N \to \infty$.

Solution

Bae and Acín solved the problem in [3], by arguing that the Choi operator of the optimal channel (for an arbitrary distribution of states) producing k indistinguishable clones must be k-extendible. By the Bolzano-Weierstrass theorem, this implies that, in finite dimensions, there exists a subsequence of optimal channels for increasing k that in the limit $k \to \infty$ tends to an ∞-extendible (and thus separable [4]) Choi matrix. Hence the channel must be entanglement-breaking and therefore of the measure-and-prepare form. In particular, the monotone sequence of values $(F(N,k))_k$ must converge to $F(N,\infty)$.

Asymptotic cloning is state estimation

Cite as: http://qig.itp.uni-hannover.de/qiproblems/22

Previous problem: Bell violation by tensoring

Next problem: SIC POVMs and Zauner's Conjecture

Contents [hide]

PRL 97, 030402 (2006) PHYSICAL REVIEW LETTERS week ending 21 JULY 2006

Asymptotic Quantum Cloning Is State Estimation

Joonwoo Bae and Antonio Acín

ICFO-Institut de Ciències Fotòniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain

(Received 15 March 2006; published 19 July 2006)

The impossibility of perfect cloning and state estimation are two fundamental results in quantum mechanics. It has been conjectured that quantum cloning becomes equivalent to state estimation in the asymptotic regime where the number of clones tends to infinity. We prove this conjecture using two known results of quantum information theory: the monogamy of quantum correlations and the properties of entanglement breaking channels.

DOI: 10.1103/PhysRevLett.97.030402 PACS numbers: 03.65.−w, 03.67.−a

m-to-n quantum cloning for qubit states

i) Universal cloning: Gisin and Massar 1997
Werner 1999
ii) Phase-covariant cloning: Bruss et al. (2000)

$$m \to n$$

quantum cloning

$$F_Q = \langle\psi|\rho^{(Q)}|\psi\rangle = \frac{nm+n+m}{n(m+2)} \xrightarrow[n\to\infty]{} \frac{m+1}{m+2}$$

$\rho^{(Q)}$

$|\psi\rangle^{\otimes m}$ $F_Q > F_M$

$$F_M = \langle\psi|\rho^{(M)}|\psi\rangle = \frac{m+1}{m+2}$$

$$F_Q^{\infty} = F_M$$

$\rho^{(M)}$

i) Universal qubit cloning:
Bruss, Ekert, and Macchiavello (1998)
ii) Universal qudit cloning:
Keyl and Werner (1999)
iii) General case:
Bae and Acin (2007);
Chiribella and D'Ariano (2007)

State estimation

Massar and Popescu 1995

Open Quantum Problems

Show 50 entries Search:

Nr	Title					
1	All the B	26	Bell inequalities holding for all quantum states	R. Gill	2010/04/19	-	Quantum foundations
		27	The power of CGLMP inequalities	R. Gill	2006/02/28	-	Quantum foundations
2	Undistill	29	Entanglement of formation for Gaussian states	O. Krüger	2005/04/20	-	Entanglement theory
		31	Individual measurement strategies on geometrically uniform states	J. Bae	2005/10/06	-	Quantum communication
4	Catalytic	32	Bell inequalities: many questions, a few answers	N. Gisin	2007/02/02	2016/12/01	Quantum foundations
5	Maxima	33	Bell inequalities and operator algebras	B. S. Tsirelson	2006/07/06	2016/06/09	Quantum foundations
8	Qubit fo of Entan	34	The geometry of quantum nonlocality	W. Slofstra and M. Navascués	2017/04/26	-	Quantum foundations
11	Continui						

Optimal Cloning of Quantum States

1980

W. K. Wootters and W. Zurek "No-Cloning Theorem" (1982)

1990

One-to-Two Universal Symmetric Qubit Cloning (V Buzek and M Hillery 1996)
General Universal Quantum Cloning (N Gisin and S Massar 1997)
Optimal Cloning (R. F. Werner 1999)
Optimal Qubit Cloning and State Estimation (D. Bruss, C. Macchiavello, A Ekert 1998,2000)

2000

Application to Quantum Key Distribution, Review on "Quantum Key Distribution"
E.g. Quantum Cryptography RMP (N Gisin, G Ribordy, W Tittel, and H. Zbinden 2002)
The Security of Practical QKD, RMP (V. Scarani et al. 2009)
Review on Quantum Cloning, (V Scarani, S. Iblisdir, N Gisin and A Acin, RMP 2005)
Asymptotic quantum cloning is state estimation (J Bae and A Acin 2006)

Story Two: Two (Bipartite) Quantum Systems

Quantum Information Theory ρ_{AB}	vs.	Information Theory p_{AB}
Qubit		Bit
Entangled bit		Secret bit
Quantum teleportation		One-time pad
Entanglement distillation		Secret key distillation
Separable states (LOCC)		Separable correlations (Public Communication)
Bound entanglement		Bound information
Quantum Shannon Theory		Shannon Theory

D Collins and S Popescu PRA 65 032321 (2002)

Entanglement is a resource

**General resource for quantum information processing,
including Quantum Computation and Secure Quantum Communication**

VOLUME 92, NUMBER 21 PHYSICAL REVIEW LETTERS week ending 28 MAY 2004

Entanglement as a Precondition for Secure Quantum Key Distribution

Marcos Curty,[1] Maciej Lewenstein,[2] and Norbert Lütkenhaus[1]

[1]*Quantum Information Theory Group, Institut für Theoretische Physik, Universität Erlangen-Nürnberg, 91058 Erlangen, Germany*
[2]*Institut für Theoretische Physik, Universität Hannover, 30167 Hannover, Germany*
(Received 21 July 2003; published 27 May 2004)

We demonstrate that a necessary precondition for an unconditionally secure quantum key distribution is that both sender and receiver can use the available measurement results to prove the presence of entanglement in a quantum state that is effectively distributed between them. One can thus systematically search for entanglement using the class of entanglement witness operators that can be constructed

PRL 94, 020501 (2005) PHYSICAL REVIEW LETTERS week ending 21 JANUARY 2005

Quantum Correlations and Secret Bits

Antonio Acín[1] and Nicolas Gisin[2]

[1]*ICFO-Institut de Ciències Fotòniques, Jordi Girona 29, Edifici Nexus II, E-08034 Barcelona, Spain*
[2]*GAP-Optique, University of Geneva, 20, Rue de l'École de Médecine, CH-1211 Geneva 4, Switzerland*
(Received 21 October 2003; published 18 January 2005)

It is shown that (i) all entangled states can be mapped by single-copy measurements into probability distributions containing secret correlations, and (ii) if a probability distribution obtained from a quantum state contains secret correlations, then this state has to be entangled. These results prove the existence of a

What is entanglement? **Quantum correlations that do not have classical counterpart**

Often, it's introduced as

SEPaprable states $\rho_{12} = \sum_i p_i \rho_i^{(1)} \otimes \rho_i^{(2)}$ ENTangled states $\rho_{12} \neq \sum_i p_i \rho_i^{(1)} \otimes \rho_i^{(2)}$

Operator-Algebraic,

Entangled states are characterised by positive (P) but not completely positive (CP) maps

$\text{Def. } \Lambda \geq 0 \text{ iff } \forall \rho \geq 0,\ \Lambda[\rho] \geq 0$

P but not CP maps $S_\Lambda = \{\Lambda : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H}) \parallel \Lambda \geq 0, \quad I \otimes \Lambda \ngeq 0\}$

$$\text{ENT} = \{\rho \in S(\mathcal{H} \otimes \mathcal{H}) \parallel (I \otimes \Lambda)[\rho] \ngeq 0,\ \Lambda \in S_\Lambda\}$$

Operationally, information-theoretically,

Entangled states are those quantum states that cannot be prepared by LOCC

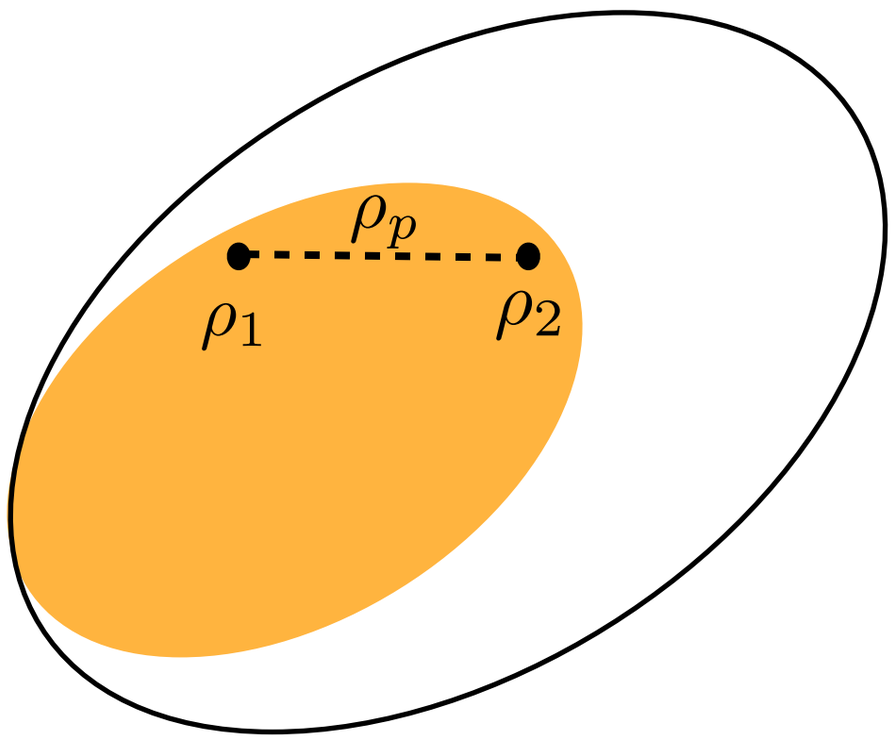
1st, in the view of quantum state preparation

Often, it's introduced as

SEPaprable states $\rho_{12} = \sum_i p_i \rho_i^{(1)} \otimes \rho_i^{(2)}$

ENTangled states $\rho_{12} \neq \sum_i p_i \rho_i^{(1)} \otimes \rho_i^{(2)}$

What can we learn? Separable states form a convex set



$$\rho_{AB} = \sum_\lambda p(\lambda) \rho_\lambda^{(A)} \otimes \rho_\lambda^{(B)}$$

$$\rho_1 \in SEP \qquad \rho_2 \in SEP$$

$$\rho_p = p\rho_1 + (1-p)\rho_2 \in SEP$$

2nd, in the view from Operator Algebra

Operator-Algebraic,

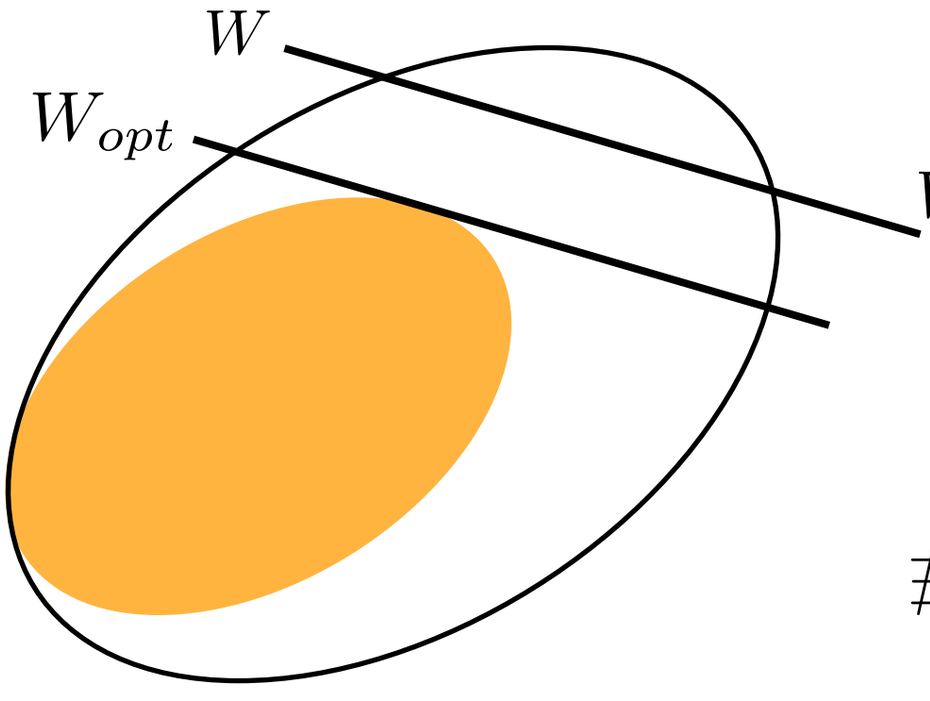
Entangled states are characterised by positive (P) but not completely positive (CP) maps

$$\text{Def.} \quad \Lambda \geq 0 \text{ iif } \forall \rho, \ \Lambda[\rho] \geq 0$$

P but not CP maps $S_\Lambda = \{\Lambda : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H}) \parallel \Lambda \geq 0, \quad I \otimes \Lambda \ngeq 0\}$

$$\text{ENT} = \{\rho \in S(\mathcal{H} \otimes \mathcal{H}) \parallel (I \otimes \Lambda)[\rho] \ngeq 0, \ \Lambda \in S_\Lambda\}$$

What can we learn? Separation of ENT from SEP: Entanglement Witnesses (EWs)



W is an entanglement witness if and only if

$$\text{tr}[\sigma W] \geq 0 \quad \forall \ \sigma \in SEP$$

$$\text{tr}[\rho W] < 0 \quad \exists \rho \in ENT$$

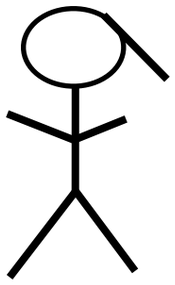
$\nexists W$ that can detect all entangled states

3rd, in the view from operational meaning

Operationally, information-theoretically,

Entangled states are those quantum states that cannot be prepared by LOCC

What can we learn? i) Power of entangled states, ii) Entangled, fully ordered

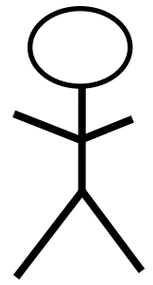


Alice

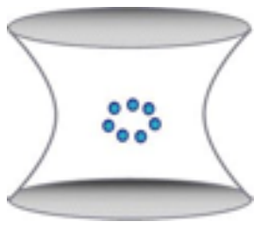
$p(\lambda) \qquad \rho_\lambda^{(A)} \otimes \rho_\lambda^{(B)}$

Classical Communication (CC)

$$\sum_\lambda p(\lambda)\rho_\lambda^{(A)} \otimes \rho_\lambda^{(B)}$$



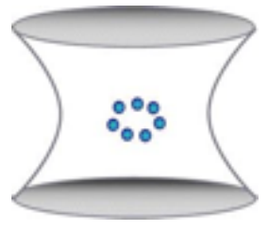
Bob



Local Operations (LO)

$$\rho_{AB} = \sum_\lambda p(\lambda)\rho_\lambda^{(A)} \otimes \rho_\lambda^{(B)} \qquad \text{Separable}$$

$$\rho_{AB} \neq \sum_\lambda p(\lambda)\rho_\lambda^{(A)} \otimes \rho_\lambda^{(B)} \qquad \text{Entangled}$$



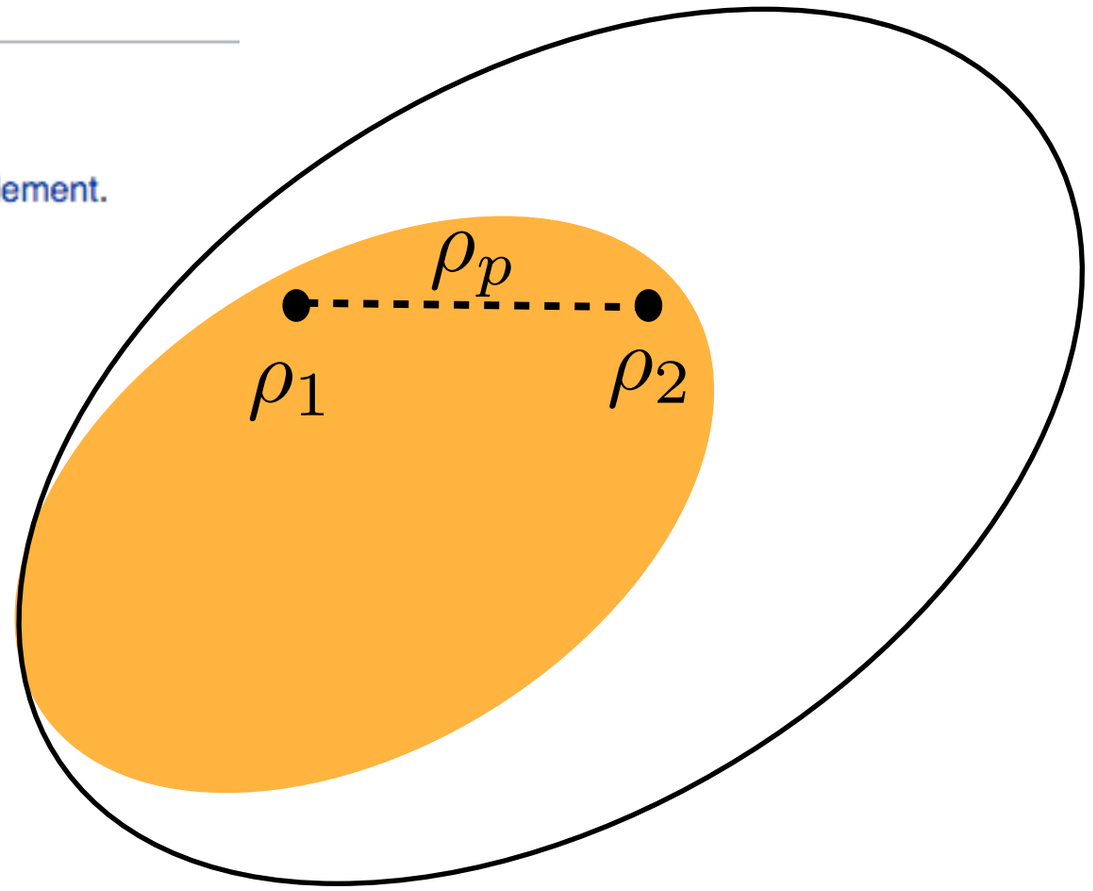
Local Operations (LO)

Separable state

From Wikipedia, the free encyclopedia

In quantum mechanics, **separable quantum states** are states without quantum entanglement.

Contents [hide]



Characterization via algebraic geometry [edit]

Quantum mechanics may be modelled on a projective Hilbert space, and the categorical product of two such spaces is th
state is separable if and only if it lies in the image of the Segre embedding. Jon Magne Leinaas, Jan Myrheim and Eirik O
entanglement"[9] describe the problem and study the geometry of the separable states as a subset of the general state m
subset of states holding Peres-Horodecki criterion. In this paper, Leinaas et al. also give a numerical approach to test for

Testing for separability [edit]

Since separability testing in a general case is an NP-hard.[1][2] problem, in their paper,[9] Leinaas et al. offer a numerical a
state towards the target state to be tested, checking if the target state can indeed be reached. An implementation of the a
testing) is brought in the "StateSeparator" web-app

General Picture of Entanglement Detection

State Preparation → quantum state verification → **Quantum State Tomography**

I don't know the state but,

want to know if it's entangled

I know the state and, (though NP-Hard)

can apply Positive Maps, SDP

Entanglement Detection → More detectors → Entangled or Separable?

Main Challenge in Quantum Information Verification: # of Measurement

$$N\ d-\text{dimensional systems} \ \rightarrow \ d^N \text{ detectors}$$

Vol 438|1 December 2005|doi:10.1038/nature04279 nature

LETTERS

Scalable multiparticle entanglement of trapped ions

H. Häffner[1,3], W. Hänsel[1], C. F. Roos[1,3], J. Benhelm[1,3], D. Chek-al-kar[1], M. Chwalla[1], T. Körber[1,3], U. D. Rapol[1,3], M. Riebe[1], P. O. Schmidt[1], C. Becher[1]†, O. Gühne[3], W. Dür[2,3] & R. Blatt[1,3]

The generation, manipulation and fundamental understanding of entanglement lies at the very heart of quantum mechanics. Entangled particles are non-interacting but are described by a common wavefunction; consequently, individual particles are not independent of each other and their quantum properties are inextricably interwoven[1–3]. The intriguing features of entanglement become particularly evident if the particles can be individually controlled and physically separated. However, both the experimental realization and characterization of entanglement

$\tau \approx 1.16$ s) represent the qubits. Each ion qubit in the linear string i individually addressed by a series of tightly focused laser pulses o the $|S\rangle \equiv S_{1/2}(m_j = -1/2) \leftrightarrow |D\rangle \equiv D_{5/2}(m_j = -1/2)$ quadrupol transition employing narrowband laser radiation near 729 nm Doppler cooling on the fast $S \leftrightarrow P$ transition (lifetime ~8 ns) an subsequent sideband cooling prepare the ion string in the groun state of the centre-of-mass vibrational mode[18]. Optical pumpin initializes the ions' electronic qubit states in the $|S\rangle$ state. Afte preparing an entangled state with a series of laser pulses, th

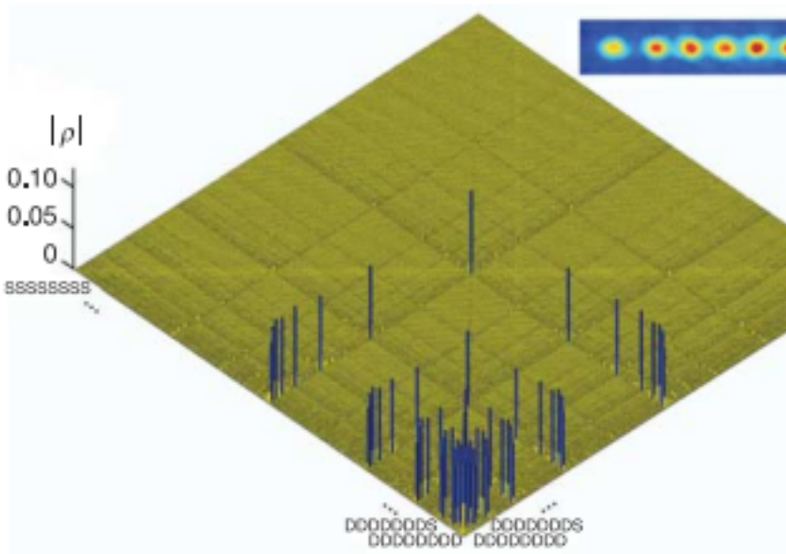


Figure 1 | Absolute values, $|\rho|$, of the reconstructed density m $|W_8\rangle$ state as obtained from quantum state tomography. DDDDDDDD…SSSSSSSS label the entries of the density matr the blue coloured entries all have the same height of 0.125; the coloured bars indicate noise. Numerical values of the density m $4 \leq N \leq 8$ can be found in Supplementary Information. In the corner a string of eight trapped ions is shown.

Table 1 | Creation of a $|W_N\rangle$-state (N = {6,7,8})

	Initialization		Entanglement
	$\lvert 0, SSS\cdots S\rangle$	(1)	$\xrightarrow{R_N^+(2\arccos(1/\sqrt{N}))}$
(i1)	$\xrightarrow{R_N^C(\pi)R_{N-1}^C(\pi)\cdots R_1^C(\pi)}$		$\frac{1}{\sqrt{N}}\lvert 0, SDD\cdots D\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}\lvert 1, DDD\cdots D\rangle$
	$\lvert 0, DDD\cdots D\rangle$	(2)	$\xrightarrow{R_{N-1}^+(2\arcsin(1/\sqrt{N-1}))}$
	Check state via fluorescence		$\frac{1}{\sqrt{N}}\lvert 0, SDD\cdots D\rangle + \frac{1}{\sqrt{N}}\lvert 0, DSD\cdots D\rangle + \frac{\sqrt{N-2}}{\sqrt{N}}\lvert 1, DDD\cdots D\rangle$
	$R_1^+(\pi)$		

Compressed sensing

From Wikipedia, the free encyclopedia

Compressed sensing (also known as **compressive sensing**, **compressive sampling**, or **sparse sampling**) is a signal processing technique for efficiently acquiring and reconstructing a signal, by finding solutions to underdetermined linear systems. This is based on the principle that, through optimization, the sparsity of a signal can be exploited to recover it from far fewer samples than required by the Shannon-Nyquist sampling theorem. There are two conditions under which recovery is possible.[1] The first one is sparsity which requires the signal to be sparse in some domain. The second one is incoherence which is applied through the isometric property which is sufficient for sparse signals.[2][3]

An early breakthrough in signal processing was the Nyquist–Shannon sampling theorem. It states that if the signal's highest frequency is less than half of the sampling rate, then the signal can be reconstructed perfectly by means of sinc interpolation. The main idea is that with prior knowledge about constraints on the signal's frequencies, fewer samples are needed to reconstruct the signal.

Around 2004, Emmanuel Candès, Terence Tao, and David Donoho proved that given knowledge about a signal's sparsity, the signal may be reconstructed with even fewer samples than the sampling theorem requires.[4][5] This idea is the basis of compressed sensing.

Quantum State Tomography via Compressed Sensing

David Gross,[1] Yi-Kai Liu,[2] Steven T. Flammia,[3] Stephen Becker,[4] and Jens Eisert[5]
[1]*Institute for Theoretical Physics, Leibniz University Hannover, 30167 Hannover, Germany*
[2]*Institute for Quantum Information, California Institute of Technology, Pasadena, California, USA*
[3]*Perimeter Institute for Theoretical Physics, Waterloo, Ontario, N2L 2Y5 Canada*
[4]*Applied and Computational Mathematics, California Institute of Technology, Pasadena, California, USA*
[5]*Institute of Physics und Astronomy, University of Potsdam, 14476 Potsdam, Germany*
(Received 21 October 2009; published 4 October 2010)

We establish methods for quantum state tomography based on compressed sensing. These methods are specialized for quantum states that are fairly pure, and they offer a significant performance improvement on large quantum systems. In particular, they are able to reconstruct an unknown density matrix of dimension d and rank r using $O(rd\log^2 d)$ measurement settings, compared to standard methods that require d^2 settings. Our methods have several features that make them amenable to experimental implementation: they require only simple Pauli measurements, use fast convex optimization, are stable

How many detectors do you need for Entanglement Detection?

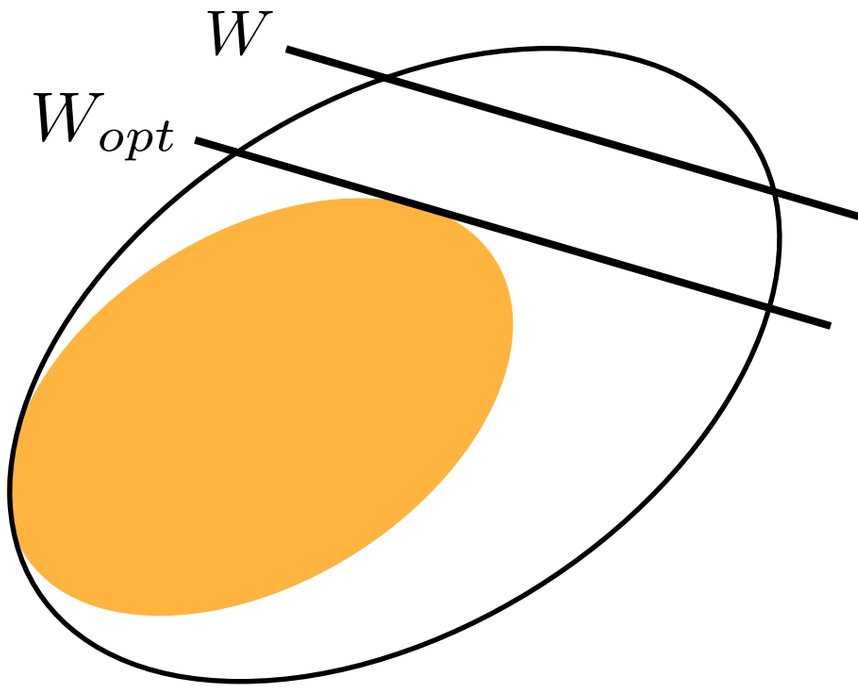
$$1 \leq \#\text{Detectors}_{\text{EW}} \leq \#\text{Detectors}_{\text{Tomography}} = d^2$$

$$\min_{\{P_i\}} \#\text{Detectors}_{\text{EWs}} = ?$$

Our contribution: Entanglement Detection with Single Hong-Ou-Mandel Interferometry

Chang Jian Kwong,[1] Simone Felicetti,[2,3] Leong Chuan Kwek,[1,4,5,6] and Joonwoo Bae[7,*]

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singap*
[2] *Department of Physical Chemistry, University of the Basque Country UPV/EHU, Apartado 644, E-48080 Bilbao, S*
[3] *Laboratoire Matériaux et Phénomènes Quantiques, Sorbonne Paris Cité, Université Paris Diderot, CNRS UMR 7162, 75013, Paris, France*
[4] *Institute of Advanced Studies, Nanyang Technological University, 60 Nanyang View, Singapore 639673, Singapor*
[5] *National Institute of Education, Nanyang Technological University, 1 Nanyang Walk, Singapore 637616, Singapor*
[6] *MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, UMI 3654, 117543, Singapore*
[7] *Department of Applied Mathematics, Hanyang University (ERICA), 55 Hanyangdaehak-ro, Ansan, Gyeonggi-do, 426-791, Korea*



W is an entanglement witness if and only if

$$\mathrm{tr}[\sigma W] \geq 0 \quad \forall \ \ \sigma \in SEP$$

$$\mathrm{tr}[\rho W] < 0 \quad \exists \rho \in ENT$$

$\nexists W$ that can detect all entangled states

Linear Transformation

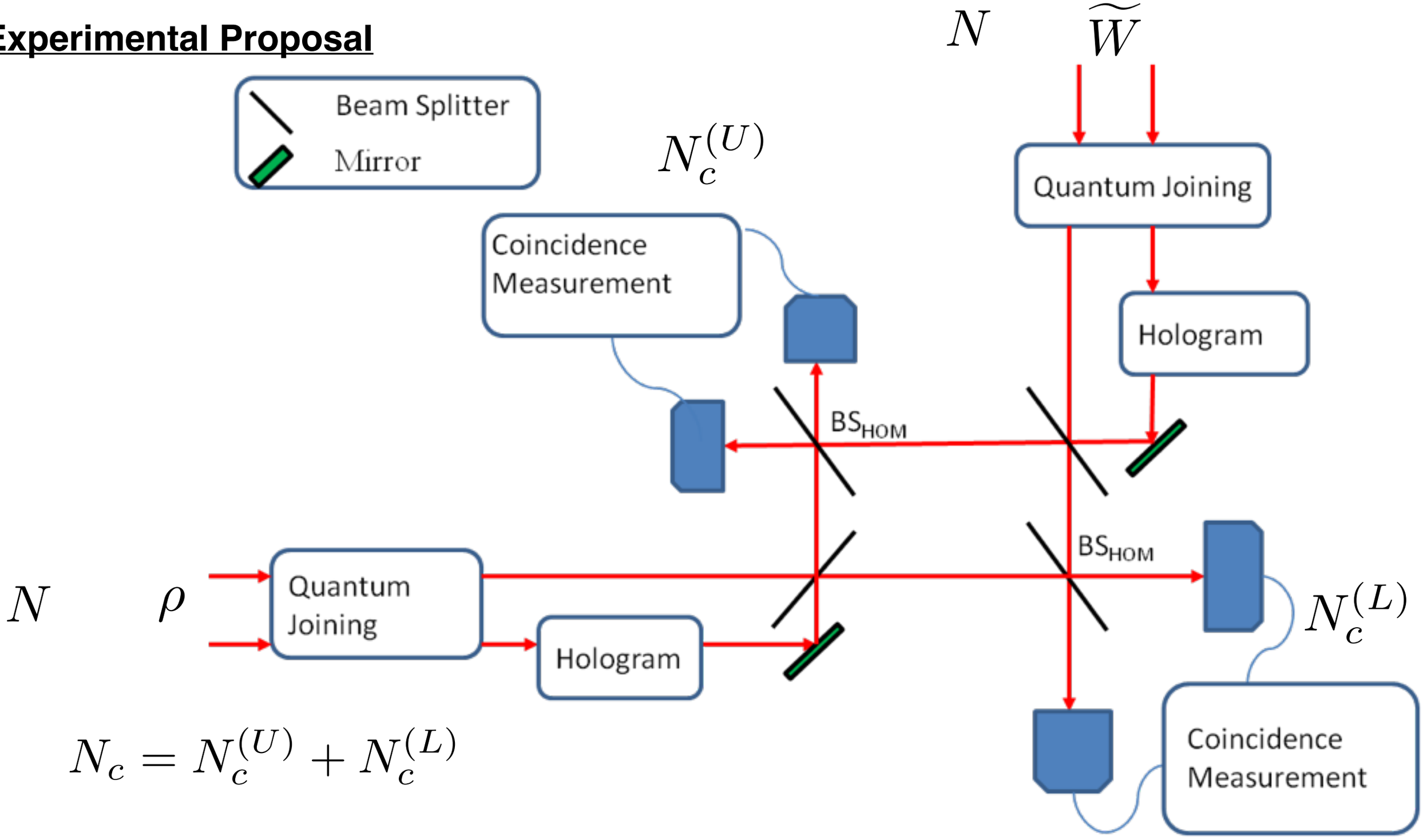
$$W \ngeq 0 \quad \longrightarrow \quad \widetilde{W} \geq 0$$

Detection Condition

$$\mathrm{tr}[W\sigma_{\mathrm{sep}}] \geq 0 \quad \longrightarrow \quad \mathrm{tr}[\widetilde{W}\sigma_{\mathrm{sep}}] \geq c^*$$

Interferometry

Experimental Proposal



$$N_c = N_c^{(U)} + N_c^{(L)}$$

$$p_c = \frac{N_c}{N/2} \quad \Rightarrow \quad \mathrm{tr}[\widetilde{W}\rho] = 1 - 2p_c$$

Story Three: Information of Three (Tripartite) Quantum Systems

but, with un-invited guy

Cryptographic Scenario

Alice

Eavesdropper

Bob

who prepares quantum states

who wants to get Alice's states while (dynamics) Alice's state evolves in time

who wants get information (in terms of bits) from quantum states (qubits) by measurement

Cryptographic Scenario

$$U \overset{\rho}{\underset{\sigma_E}{\otimes}} U^\dagger$$

$\rho_A \in S(\mathcal{H}_A)$ → **Quantum channel** → $\rho_B \in S(\mathcal{H}_B)$

$$\Lambda_B[\rho_A] = \mathrm{tr}_E[U(\rho_A \otimes \sigma_E)U^\dagger]$$

Complementary channel

$$\Lambda_E[\rho_A] = \mathrm{tr}_A[U(\rho_A \otimes \sigma_E)U^\dagger]$$

History of Cryptography

1926 — One-Time Pad (Vernam cipher)

2nd World War — Significance of cryptographic systems

1948 — Shannon's proof: perfect secrecy of one-time pad

1977 — DES/AES:
Private-key systems / Symmetric keys
Rivest, Shamir, Adleman (RSA), Diffie-Hellman:
Public-key systems / Asymmetric keys

Commercialised

Modern Cryptography: development of security analysis

-**defining security: parameters / assumptions**
-hash functions
-random generators
-computational models: computational complexity, e.g. P=NP?

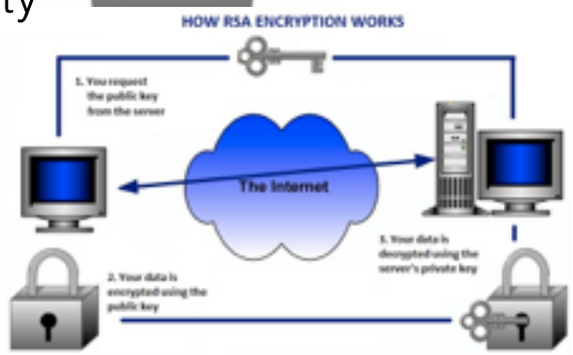
1994,8 — Shor's factorisation algorithm in quantum computation

<u>On Security</u>: Reductionist's approach What do we mean by proving security?

Step 1: Define security **Keyword: Assumptions, Security**

Step 2: Explain correspondence to implementation and elements of security

Step 3: REDUCE the analysis to its ultimate equivalence to the definition of security



Rivest, Shamir, Adleman (RSA): Public-key systems / Asymmetric keys

Security of public-key systems ⟷ Factorisation Problem: Factorisation of BIG numbers

How hard is it to solve the factorisation problem?

ex. 251 * 479 = 120,229, >100 digits, +100 yrs

Complexity of factorisation (**computational security**) is unknown yet. (**Unproven assumption**)

One-time pad contains perfect security: Shannon inf-theoretic, symmetric keys, private-key systems.

provable security! **(Information-theoretic security)**

Security of private-key systems ⟷ **Secret Key**

Alice	Bob	$\forall$ Eve	Probability
0	0	e	$1/2$
1	1	e	$1/2$

If quantum computation is realised, quantum algorithms…

CAN SOLVE FACTORISATION PROBLEM IN AN EFFICIENT WAY.

‘key idea of RSA protocols’

NEW CRYPTOGRAPHIC PROTOCOLS: QUANTUM CRYPTOGRAPHY

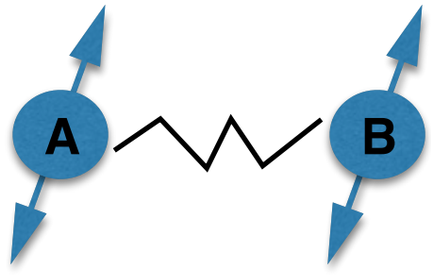
Peter Shor in 1995, recipient of Nevanlinna Prize (1998)

IT’S POSSIBLE TO IMPLEMENT QUANTUM COMPUTERS

I. Cirac and P. Zoller in 1995, recipients of Wolf Prize (2013)

Entanglement means security

$$\phi^+ = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$



$$\phi^+ = \vec{\phi}\vec{\phi}^\dagger \qquad \vec{\phi} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \qquad \phi^+ \in S(\mathcal{H}_A \otimes \mathcal{H}_B)$$

$$\exists ? \rho_{ABE}, \text{ such that } \mathrm{tr}_E \rho_{ABE} = \phi^+_{AB} \longrightarrow \rho_{ABE} = \phi^+_{AB} \otimes \rho_E$$

$$p_{ABC}(x,y,z|a,b,c) = \mathrm{tr}[\rho_{ABC} M^a_x \otimes M^b_y \otimes M^c_z] = \mathrm{tr}[\phi^+_{AB} \otimes \rho_C M^a_x \otimes M^b_y \otimes M^c_z$$
$$= \mathrm{tr}[\phi^+_{AB} M^a_x \otimes M^b_y]\mathrm{tr}[\rho_C M^c_z] = p_{AB}(x,y|a,b)p_C(z|c)$$

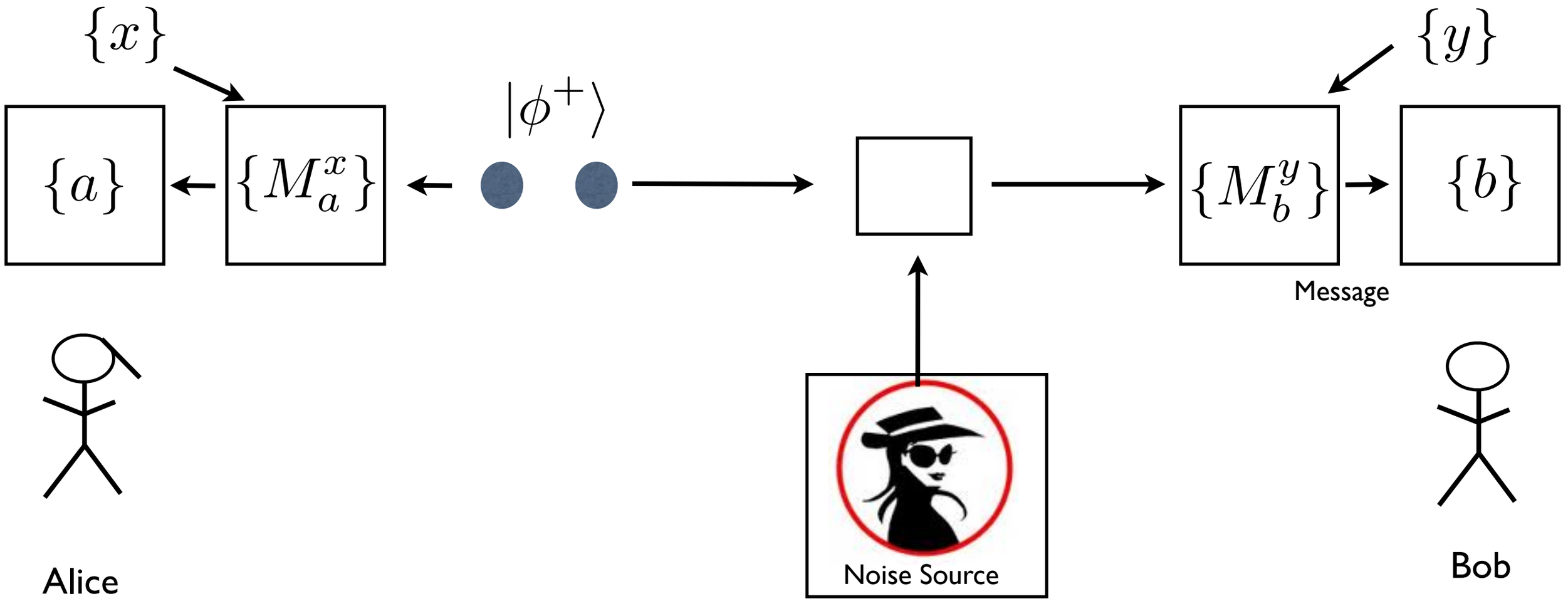
$$\longrightarrow I(A,B:C) = 0$$

Parties AB are completely independent with any other C!

Alice	Bob	$\forall$ Eve	Probability
0	0	e	1/2
1	1	e	1/2

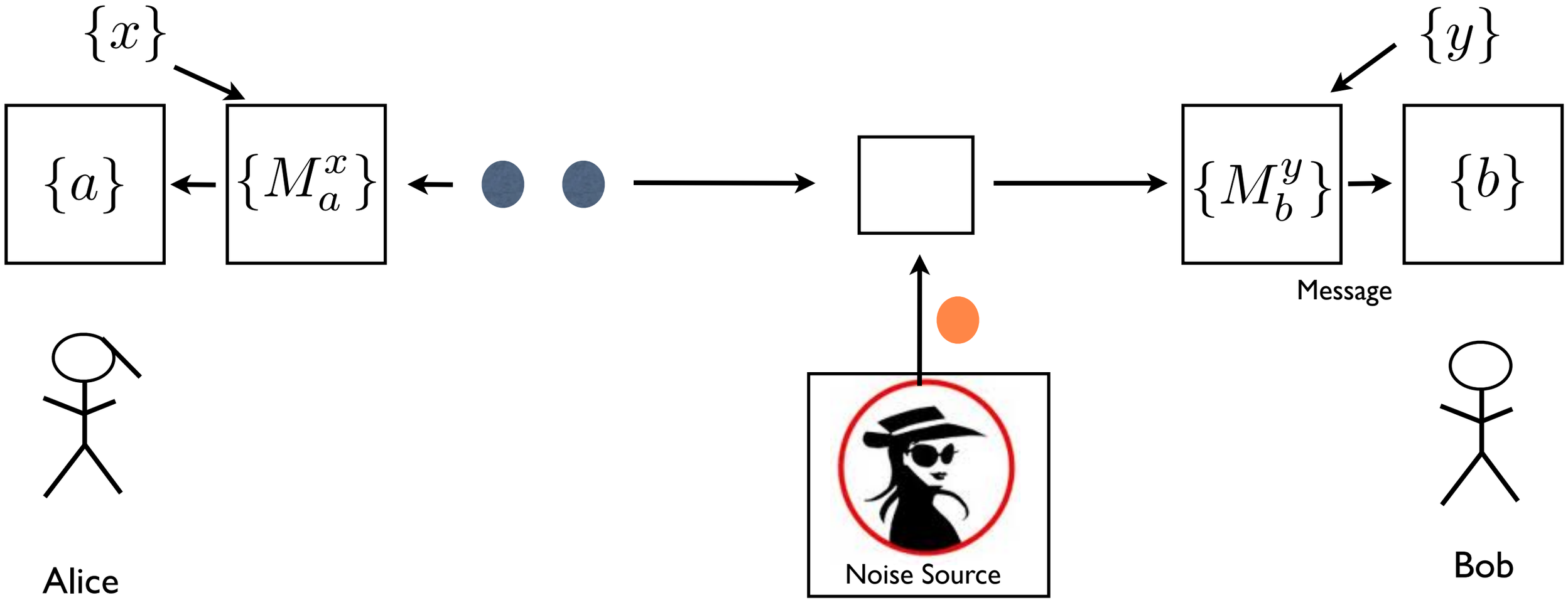
Quantum Communication Scenario

$$|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$



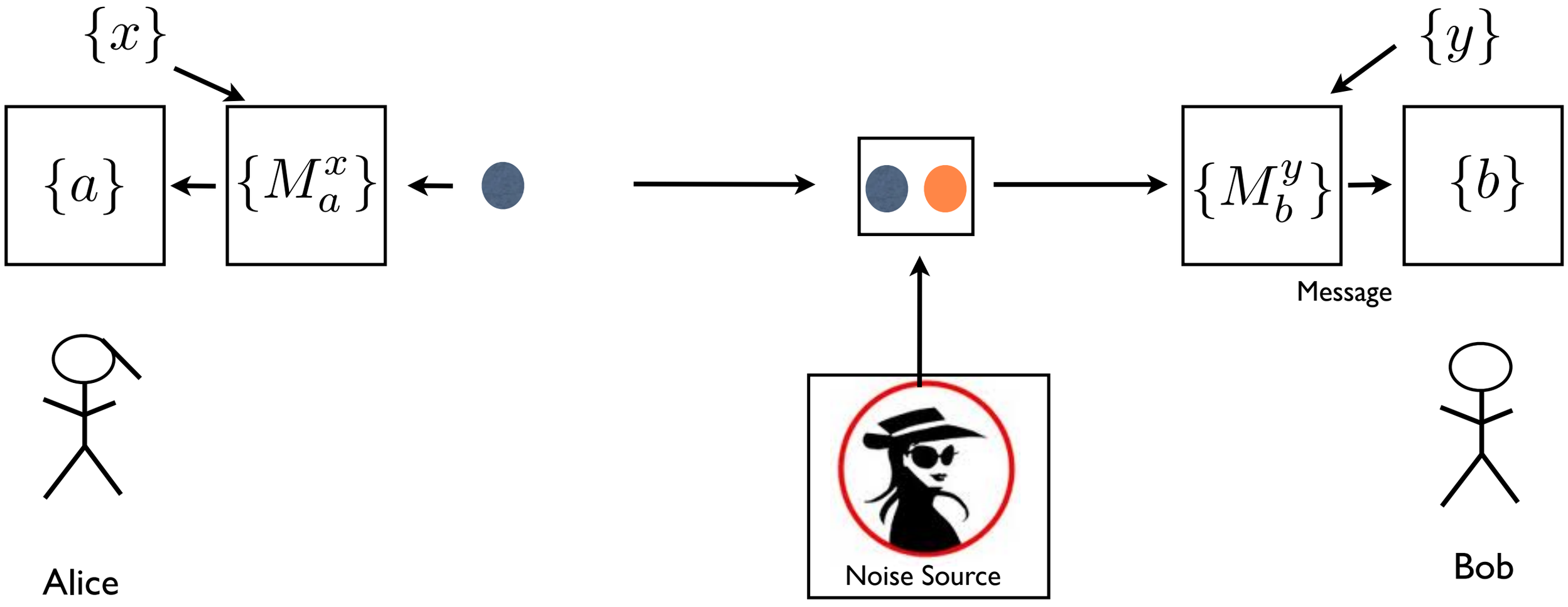
Quantum Communication Scenario

$$|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$



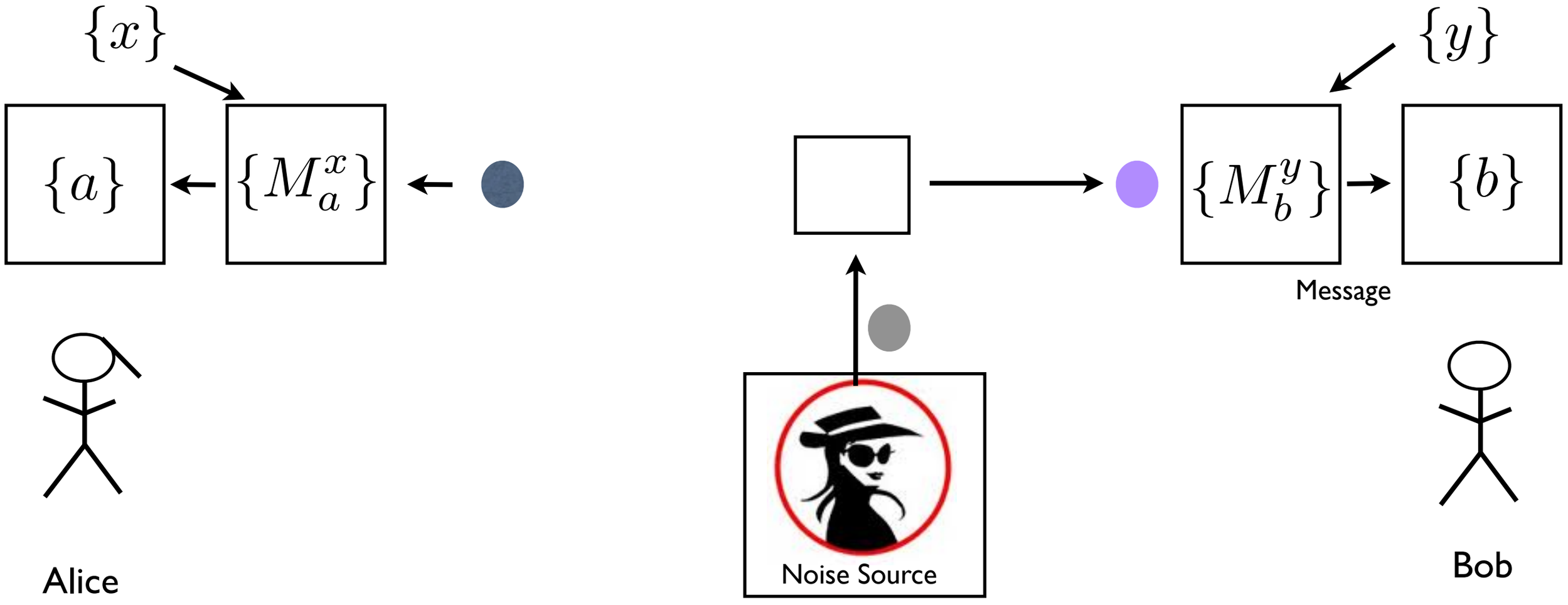
Quantum Communication Scenario

$$|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$



Quantum Communication Scenario

$$|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$



Quantum cloning without signaling

N. Gisin

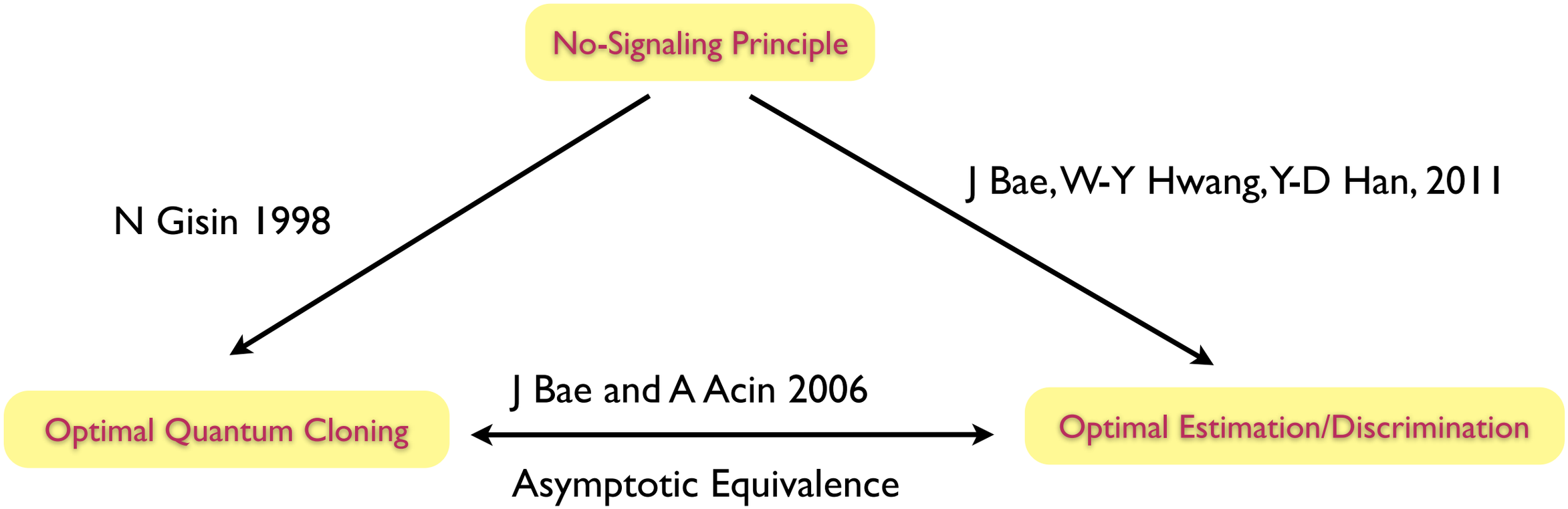
Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland

Received 26 January 1998; accepted for publication 25 February 1998
Communicated by P.R. Holland

Abstract

Perfect quantum cloning machines (QCM) would allow one to use quantum non-locality for arbitrary fast signaling. However, perfect QCM cannot exist. We derive a bound on the fidelity of QCM compatible with the no-signaling constraint. This bound equals the fidelity of the Bužek–Hillery QCM. © 1998 Elsevier Science B.V.

"Perfect quantum cloning would allow one to use quantum non-locality for arbitrary fast signaling"



PRL **107,** 170403 (2011) PHYSICAL REVIEW LETTERS week ending 21 OCTOBER 2011

No-Signaling Principle Can Determine Optimal Quantum State Discrimination

Joonwoo Bae,[1,*] Won-Young Hwang,[2] and Yeong-Deok Han[3]

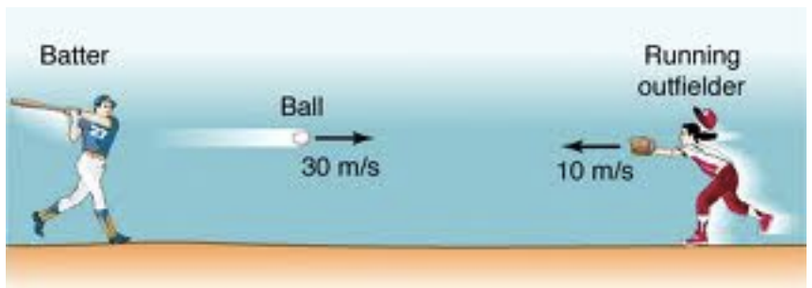
[1]*School of Computational Sciences, Korea Institute for Advanced Study, Seoul, 130-012, Republic of Korea*
[2]*Department of Physics Education, Chonnam National University, Gwangju 500-757, Republic of Korea*
[3]*Department of Game Contents, Woosuk University, Wanju, Cheonbuk 565-701, Republic of Korea*
(Received 7 March 2011; published 20 October 2011)

We provide a general framework of utilizing the no-signaling principle in derivation of the guessing probability in the minimum-error quantum state discrimination. We show that, remarkably, the guessing

Security of Quantum Cryptography: Quantum theory governs Nature!

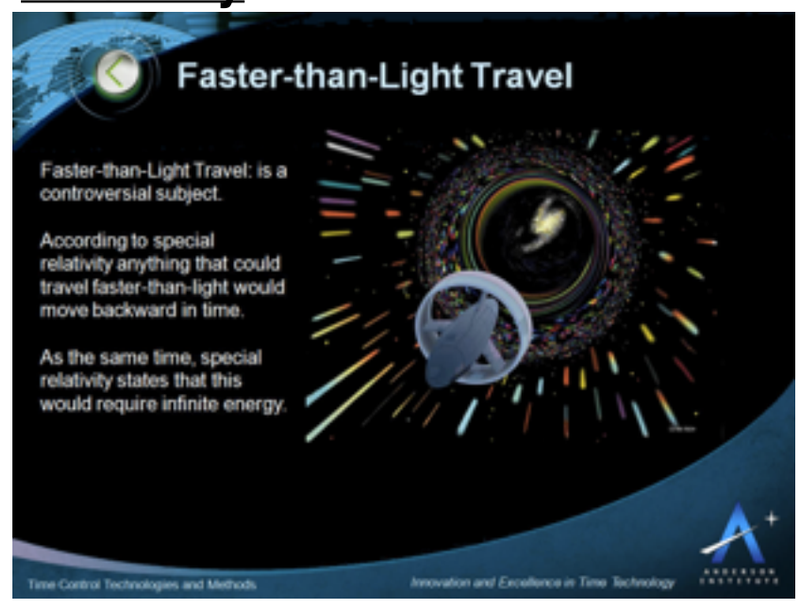
Quantum mechanics is tightly connected to Relativity

Newton's mechanics



As seen by outfielder, ball is approaching her at
(30 m/s) + (10 m/s) = 40 m/s
a

Relativity



Quantum Mechanics in 1 Slide

Classical Probability:

$$\begin{pmatrix} s_{11} & \cdots & s_{1n} \\ \vdots & \ddots & \vdots \\ s_{n1} & \cdots & s_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} = \begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix}$$

$$p_i \geq 0, \quad \sum_{i=1}^{n} p_i = 1$$

Can apply linear transformations that conserve 1-norm of *probability* vectors

Quantum Mechanics:

$$\begin{pmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & \ddots & \vdots \\ u_{n1} & \cdots & u_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

$$\alpha_i \in \mathbb{C}, \quad \sum_{i=1}^{n} |\alpha_i|^2 = 1$$

Can apply linear transformations that conserve 2-norm of *amplitude* vectors

Research in quantum cryptography: The principle is secure but its implementation is insecure.

Grover Search and the No-Signaling Principle

Ning Bao
Institute for Quantum Information and Matter and Walter Burke Institute for Theoretical Physics, California Institute of Technology 452-48, Pasadena, California 91125, USA

Adam Bouland
Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

SECTION G: OPEN PROBLEMS

We have shown that in several domains of modifications of quantum mechanics, the resources required to observe superluminal signaling or a speedup over Grover's algorithm are polynomially related. We extrapolate that this relationship holds more generally, that is, in any quantum-like theory, the Grover lower bound is derivable from the no-signaling principle and vice-versa. A further hint in this direction is that, as shown in [30], the limit on distinguishing non-orthogonal states in quantum mechanics is dictated by the no-signaling principle. Thus, any improvement over the Grover lower bound based on beyond-quantum state discrimination can be expected to imply some nonzero capacity for superluminal signaling. There is a substantial literature on generalizations of quantum mechanics which could be drawn upon to address this question. In particular, one could consider the generalized probabilistic theories framework of Barrett [31], the category-theoretic framework of Abramsky and Coecke [32], the Newton-Schrödinger equation [33], quaternionic quantum mechanics [34], or the Papadodimas-Raju state-dependence model of black hole dynamics [17, 18, 35]. In these cases the investigation of computational and communication properties is inseparably tied with the fundamental questions about the physical interpretations of these models. Possibly, such investigation could help shed light on these fundamental questions.

Grover Search and the No-Signaling Principle

Ning Bao
Institute for Quantum Information and Matter and Walter Burke Institute for Theoretical Physics, California Institute of Technology 452-48, Pasadena, California 91125, USA

Adam Bouland
Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

SECTION G: OPEN PROBLEMS

We have shown
to observe superlu
trapolate that this
bound is derivable
as shown in [30],
the no-signaling pr
state discriminatio
a substantial litera
this question. In
rett [31], the categ
[33], quaternionic
dynamics [17, 18,
inseparably tied wi
such investigation

[27] Childs, A. M. & Young, J. Optimal state discrimination and unstructured search in nonlinear quantum mechanics (2015). ArXiv:1507.06334.
[28] Wigner, E. P. *Gruppentheorie und ihre Anwendung auf die Quanten mechanik der Atomspektren*, 251–254 (Friedrich Vieweg und Sohn, 1931).
[29] Aharonov, D. A simple proof that Toffoli and Hadamard are quantum universal (2003). ArXiv:quant-ph/0301040.
[30] Bae, J., Hwang, W.-Y. & Han, Y.-D. No-signaling principle can determine optimal quantum state discrimination. *Physical Review Letters* **107**, 170403 (2011). ArXiv:1102.0361.
[31] Barrett, J. Information processing in generalized probabilistic theories. *Physical Review A* **75**, 032304 (2005). ArXiv:quant-ph/0508211.
[32] Abramsky, S. & Coecke, B. Categorical quantum mechanics. In Engesser, K., Gabbay, D. & Lehmann, D. (eds.) *Handbook of Quantum Logic and Quantum Structures*, vol. 2, 261–325 (Elsevier, 2008). ArXiv:0808.1023.
[33] Ruffini, R. & Bonazzola, S. Systems of self-gravitating particles in general relativity and the concept of an equation of state. *Physical Review* **187**, 1767 (1969).
[34] Adler, S. L. *Quaternionic Quantum Mechanics and Quantum Fields* (Oxford University Press, Oxford, 1995).
[35] Harlow, D. Aspects of the Papadodimas-Raju proposal for the black hole interior. *Journal of High Energy Physics* 1411 (2014). ArXiv:1405.1995.
[36] Brun, T. Computers with closed timelike curves can solve hard problems. *Foundations of Physics Letters* **16**, 245–253 (2003). ArXiv:gr-qc/0209061.
[37] Harlow, D. & Hayden, P. Quantum computation vs. firewalls. *Journal of High Energy Physics* **1013:85** (2013). ArXiv:1301.4504.
[38] Harlow, D. Personal communication .

Learning from the history

1930 1940 1960 1990

C. Helstrom, A. Holevo, H. Yuen, Lax, and Kenney (1974-6)

W. K. Wootters and W. Zurek, "A single quantum cannot be cloned" Nature 229 802 (1982)

J. I. Cirac and P. Zoller, "Quantum Computation with Cold Trapped Ions" PRL 74 4091 (1995)

Quantum Signal Processing

No-Cloning Theorem

Quantum State Engineering

BB84
C. H. Bennett and G. Brassard, "Quantum Cryptography", Bangalore (1984)

J. Bell, Physics 1, 195 (1965)

Bell's Theorem, Non-Locality

A. Ekert
"Quantum cryptography based on Bell's theorem", PRL 67 661 (1991)

Quantum Cryptography

A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. 47, 777 (1935)

E. Schroedinger and M. Born (1935) - "Entanglement"

Entanglement, Steering

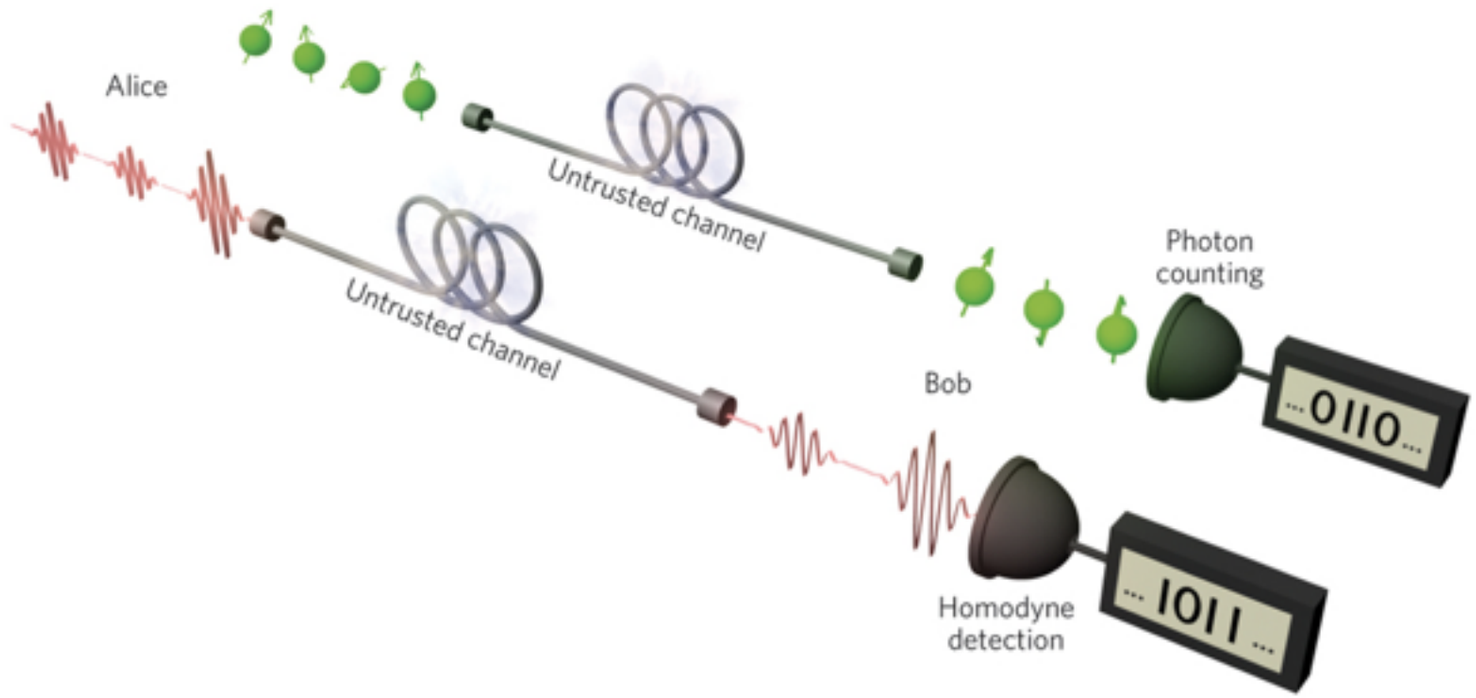
C. H. Bennett, G. Brassard, and D. Mermin, "Quantum cryptography without Bell's theorem" PRL (1992)

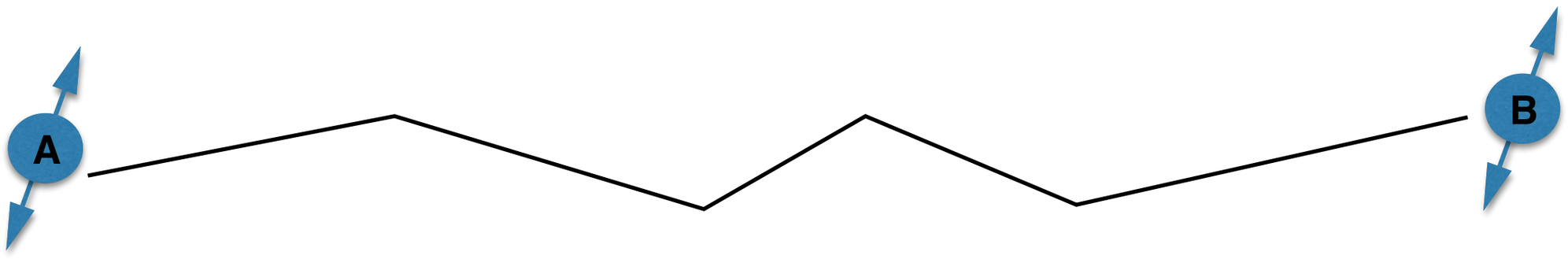
Quantum Cryptography in Practice

- On-Going and Future Direction -

Quantum Cryptographic Scenario

$$\phi^+ = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$





An unbreakable code

Quantum key encryption gives computer security a random code key that hackers can't crack. It relies on individual light particles called photons that stream over a fiber-optic line from one computer to another. How it works:

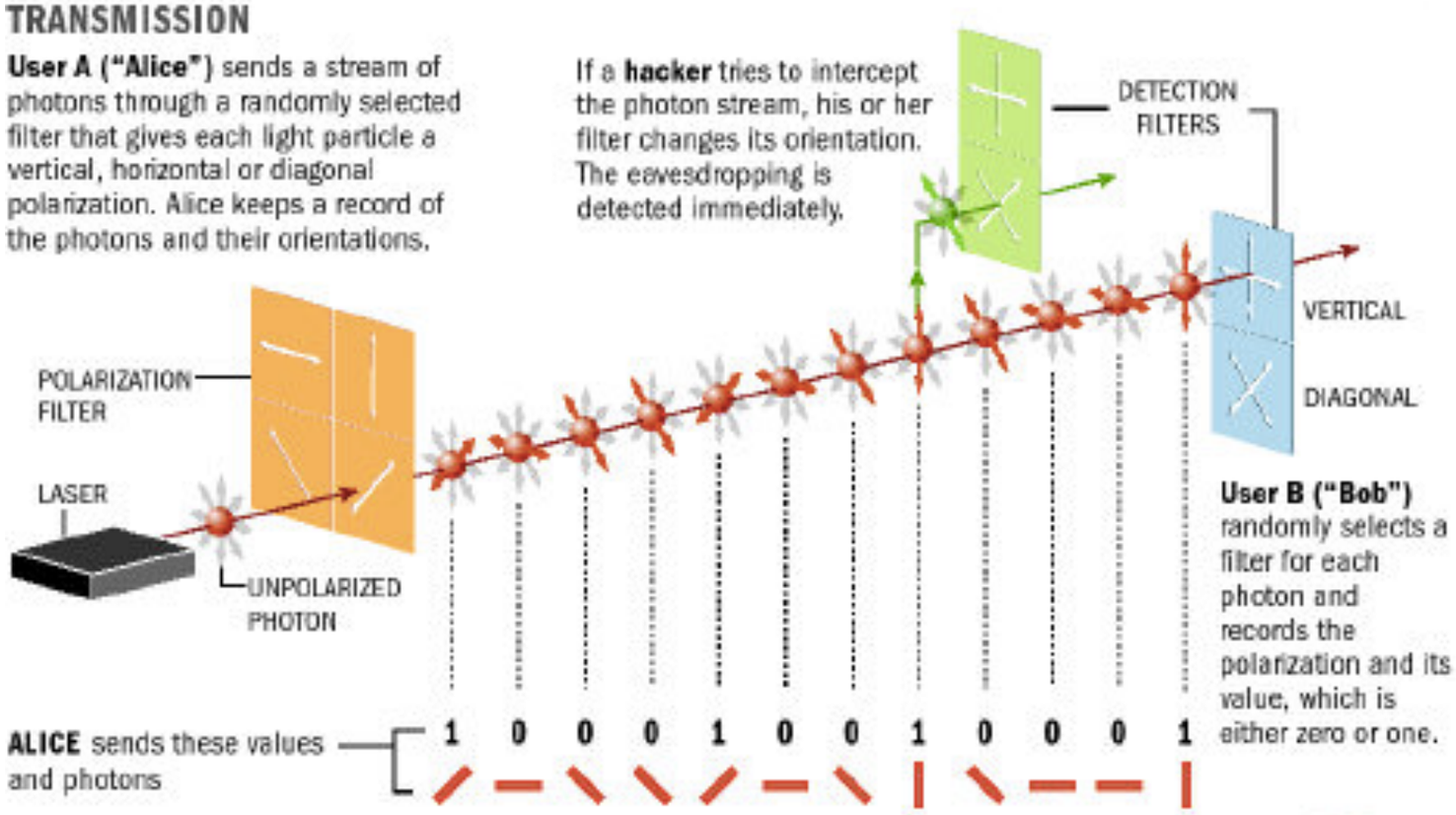
KEY VALUES

POLARIZATION	PHOTONS	
Rectilinear		
Diagonal		
ESTABLISHED BIT VALUE	0	1

TRANSMISSION

User A ("Alice") sends a stream of photons through a randomly selected filter that gives each light particle a vertical, horizontal or diagonal polarization. Alice keeps a record of the photons and their orientations.

If a **hacker** tries to intercept the photon stream, his or her filter changes its orientation. The eavesdropping is detected immediately.



User B ("Bob") randomly selects a filter for each photon and records the polarization and its value, which is either zero or one.

ALICE sends these values and photons

1 0 0 0 1 0 0 1 0 0 0 1

BOB detects these values and photons; note that the photons are not all detected correctly.

1 0 1 0 1 1 0 1 0 0 0 1

SHARED SEQUENCE

This communication takes place over a public channel.

Bob tells Alice which filters he used, but not each photon's value. Alice informs Bob which measurements were made with the incorrect filter. The remaining bits form the encryption key.

ENCRYPTION KEY 1 0 … 0 … … 0 1 0 … 0 1

Sources: Battelle; *Scientific American*

MARY T. NGUYEN | DISPATCH

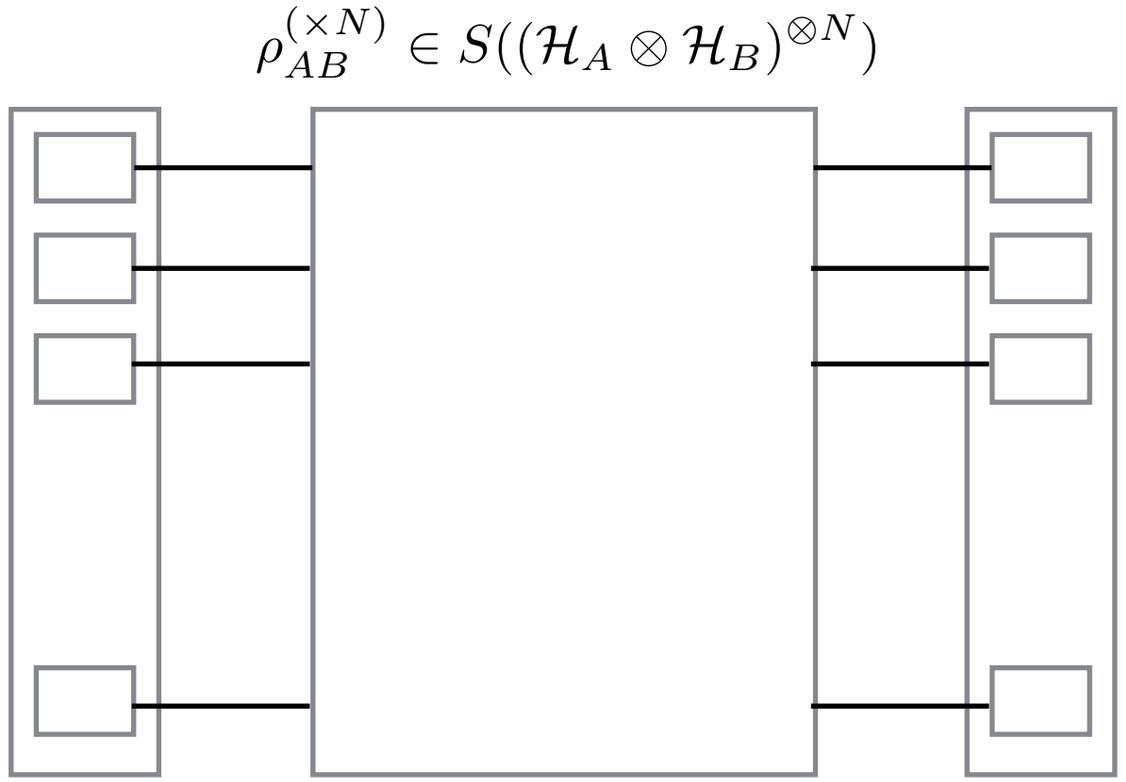
$\mathcal{B}(\mathcal{H})$ bounded operators

$\mathcal{S}(\mathcal{H})$ quantum states $\rho \geq 0 \quad \mathrm{tr}\rho = 1$

Quantum Cryptographic Scenario $\rho_{ABE}^{(\times N)}$

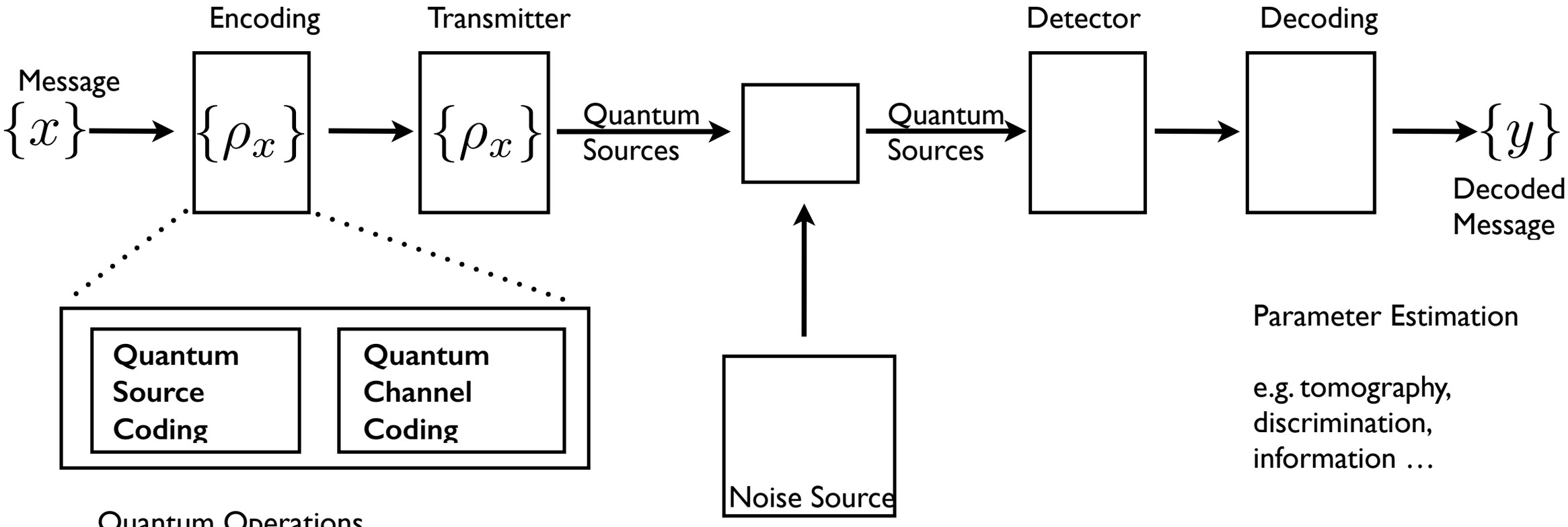
Entanglement-based scheme:

$$\rho_{ABE}^{(\times N)} = (\mathrm{id}_A \otimes \Lambda_{BE}^{(N)})[|\phi_+\rangle_{AB}\langle\phi^+|^{\otimes N} \otimes |0\rangle_E\langle 0||]$$



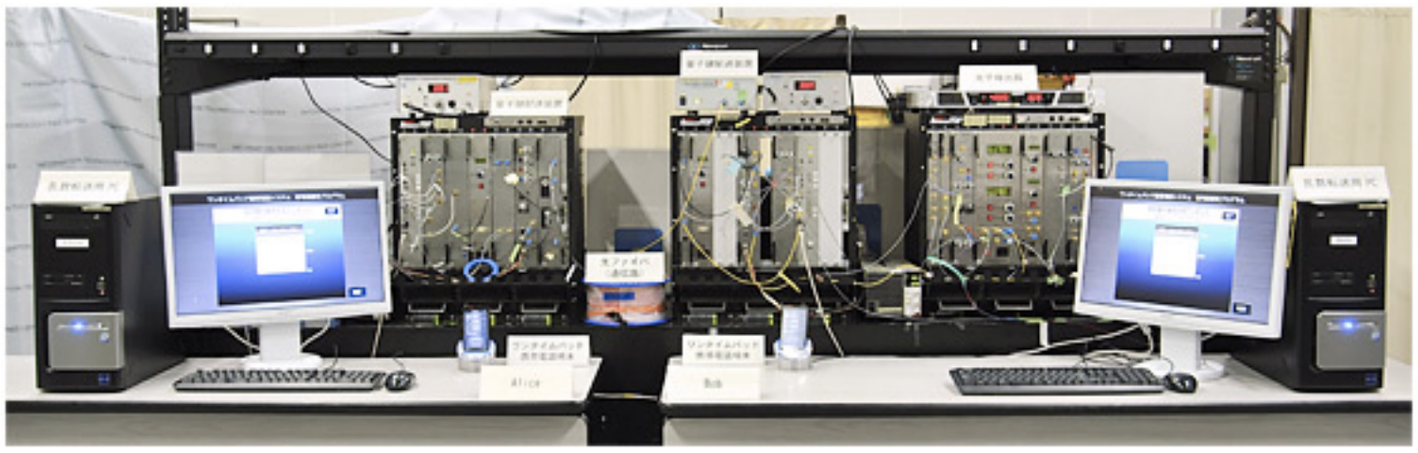
Secret-key distillation protocol: $\Lambda_{AB}^{(KD)}$
Local Operation and Public Communication (LOPC)

$$K_D(A:B\|E) = \sup_{N,\Lambda_{AB}^{(KD)}} \frac{\#\mathrm{sbit}}{N}$$



Quantum Operations

$$\mathcal{B}(\mathcal{H}^{\otimes N}) \to \mathcal{B}(\mathcal{H}^{\otimes M})$$



i) **Preparation** of quantum states

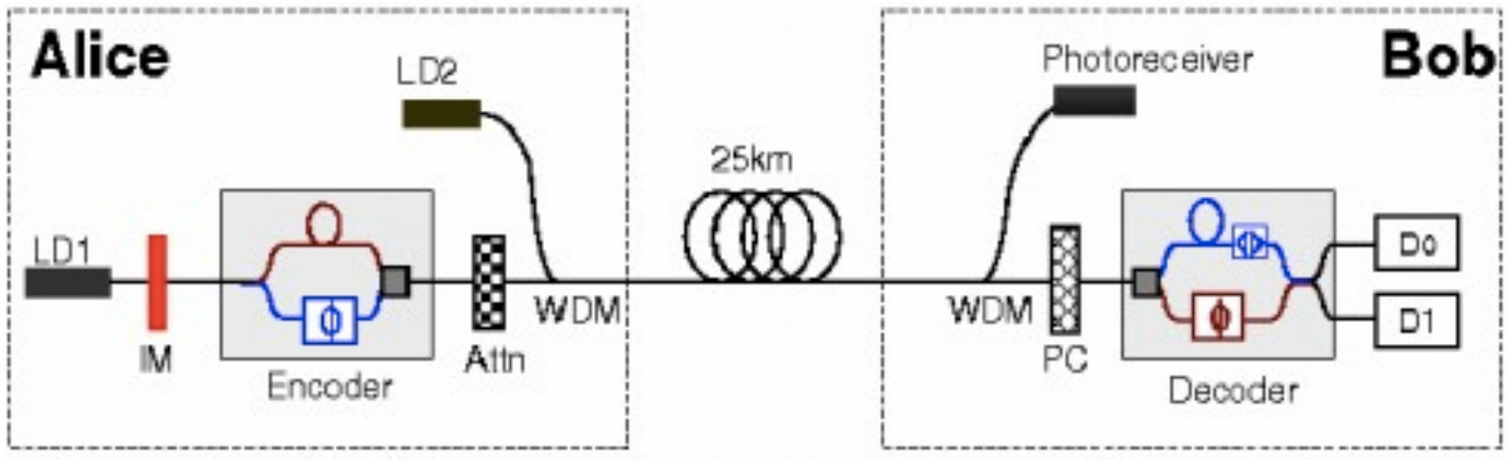
ii) **Transmission** of quantum states

iii) **Detection/Measurement** of quantum states

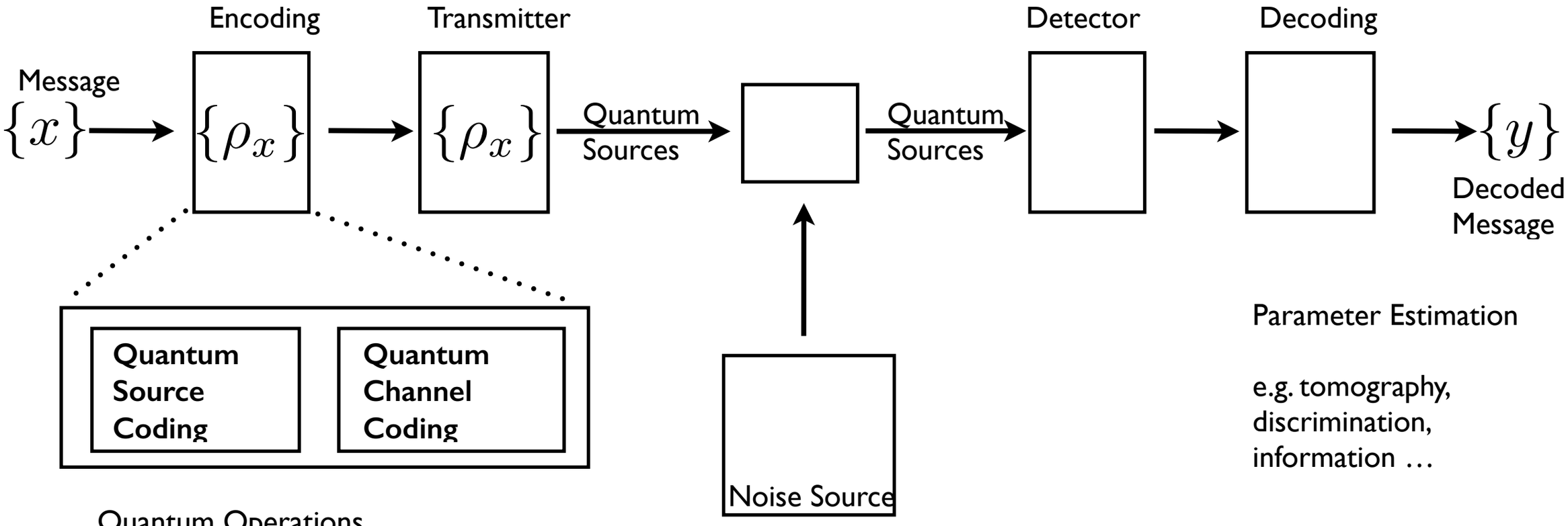
iv) Post-processing (parameter-estimation, key-distillation, error-correction, privacy amplification.)
- Quantum Information Theory Tools

Quantum Systems: Systems governed by the laws of quantum mechanics

Ex. Atoms, Electrons, Photons, …

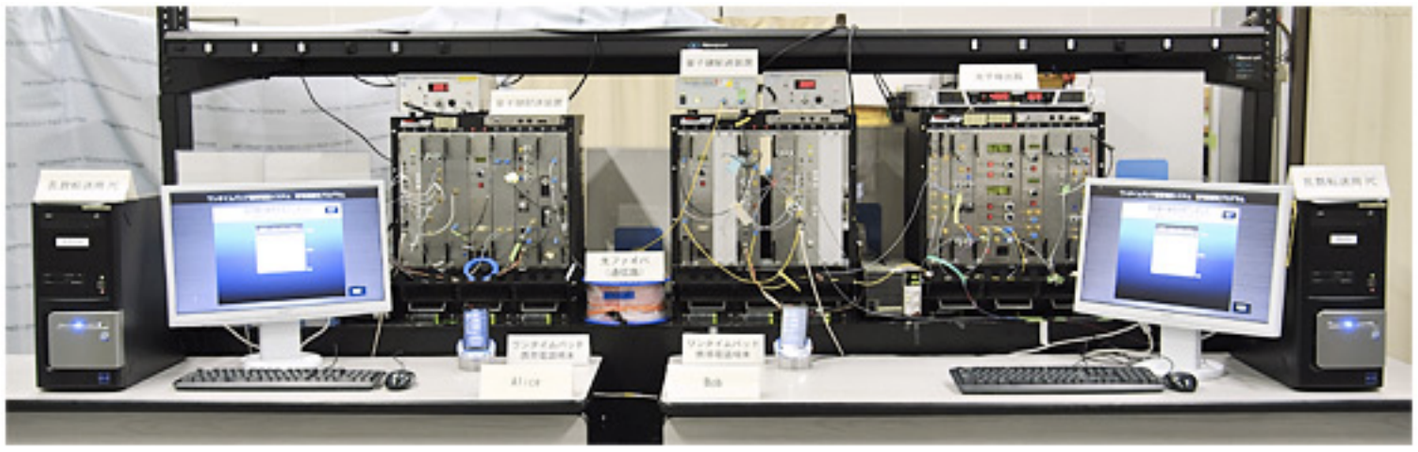


quantum systems for long-distance communication: photons, hardly interacting during transmission



Quantum Operations

$$\mathcal{B}(\mathcal{H}^{\otimes N}) \to \mathcal{B}(\mathcal{H}^{\otimes M})$$



i) **Preparation** of quantum states

ii) **Transmission** of quantum states

iii) **Detection/Measurement** of quantum states

iv) Post-processing (parameter-estimation, key-distillation, error-correction, privacy amplification.)
- Quantum Information Theory Tools

History of Quantum Cryptography

1994,8 — Shor's factorisation algorithm in quantum computation
RSA reserved to be broken

2000 — The first security proof (Shor, Preskill): < 11%
channel noise

2003,4 — Decoy QKD (Hwang)
SARG04 (Geneva),
source preparation
The problem of single photon sources

2007 — The Most general security proof
(Bae, Acin)
channel noise
The highest error-rate

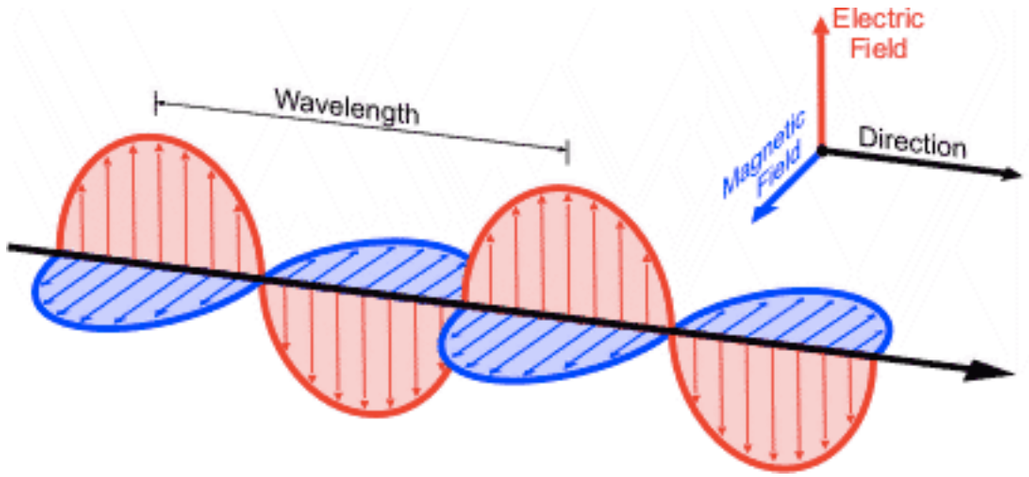
2011 — Measurement-Device-Independent (MDI) QKD
detector problems
Security not yet fully proven

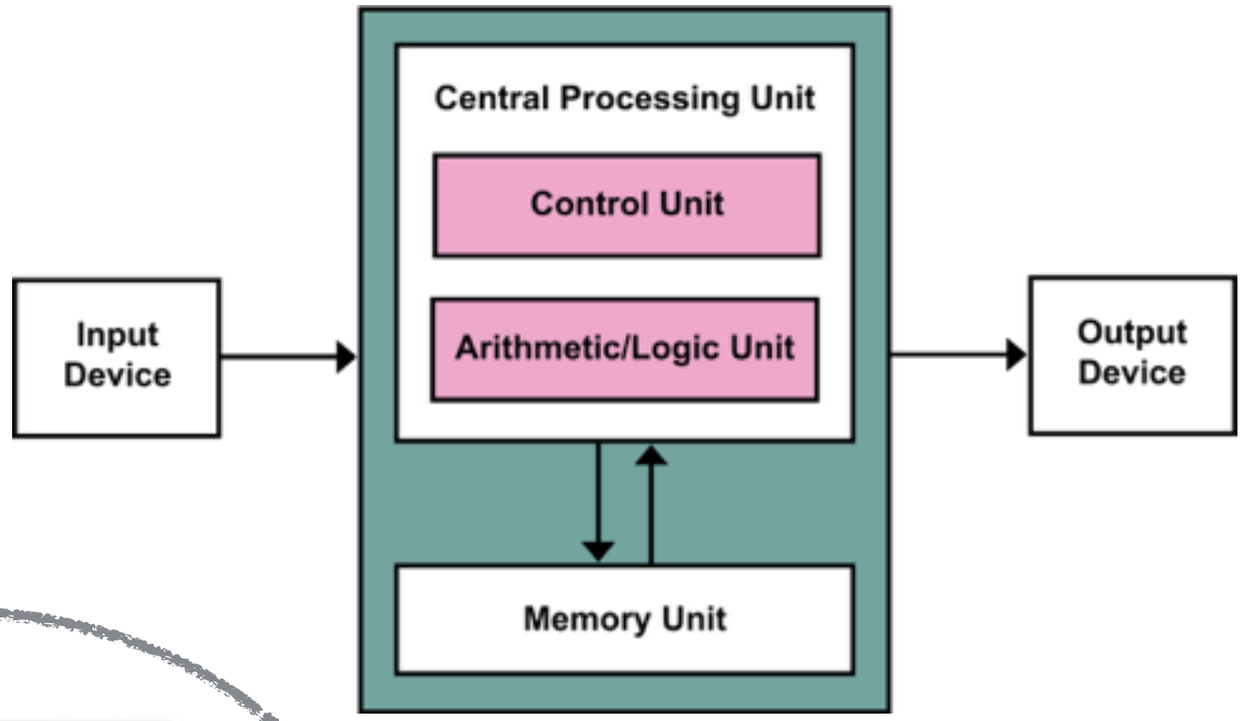
2014 — Device-Independent QKD
detector problems
can tolerate 1% error-rate

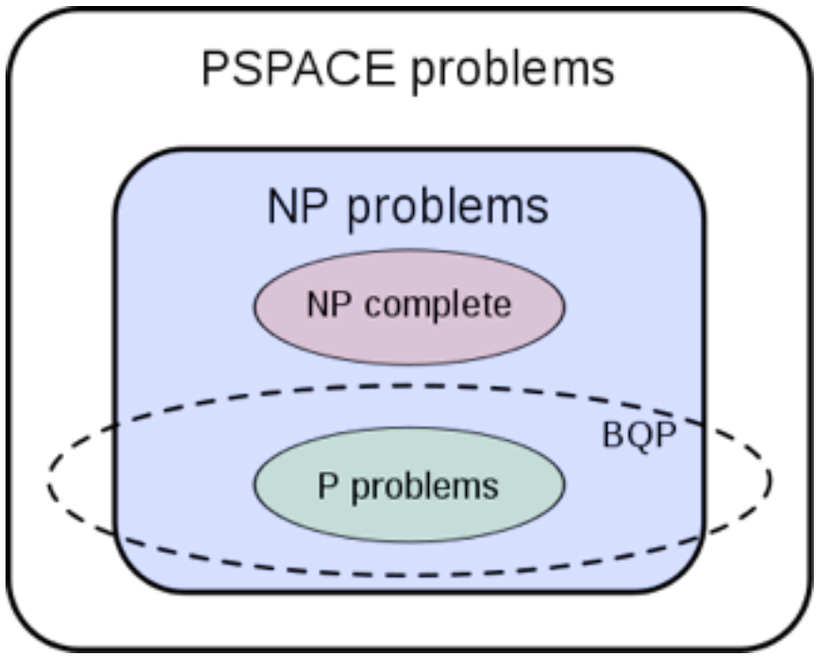
2016 — Future direction:
New QKD protocols
source,channel,detectors
compassable security
realistic security
Composable
Realistic security

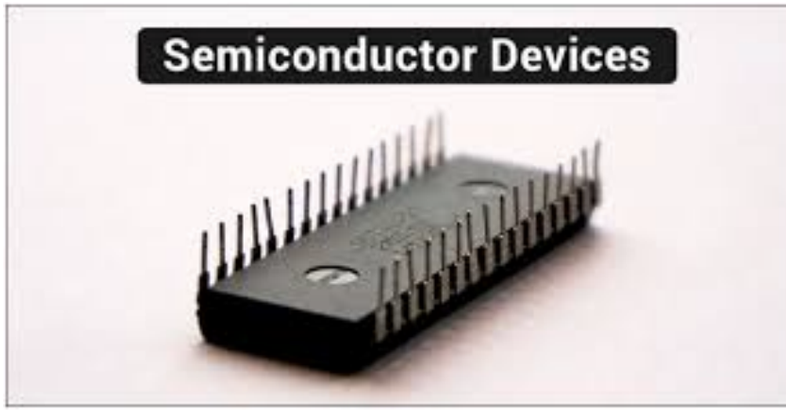
Quantum Computer, Quantum Evolution, and Quantum Simulation

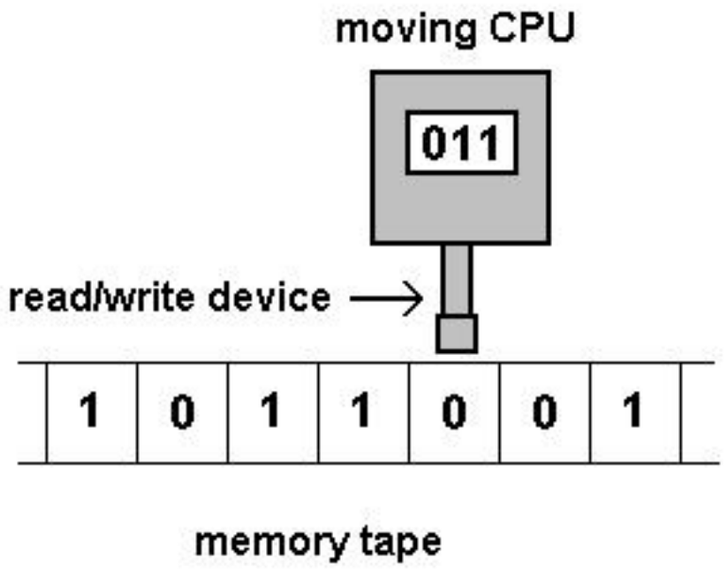
The Next Story: Information of Many Quantum Systems
THE BEGINNING OF THE NEXT, TOWARD BLUE SKY RESEARCH


Wavelength
Electric Field
Magnetic Field
Direction


Central Processing Unit
Control Unit
Arithmetic/Logic Unit
Input Device
Output Device
Memory Unit

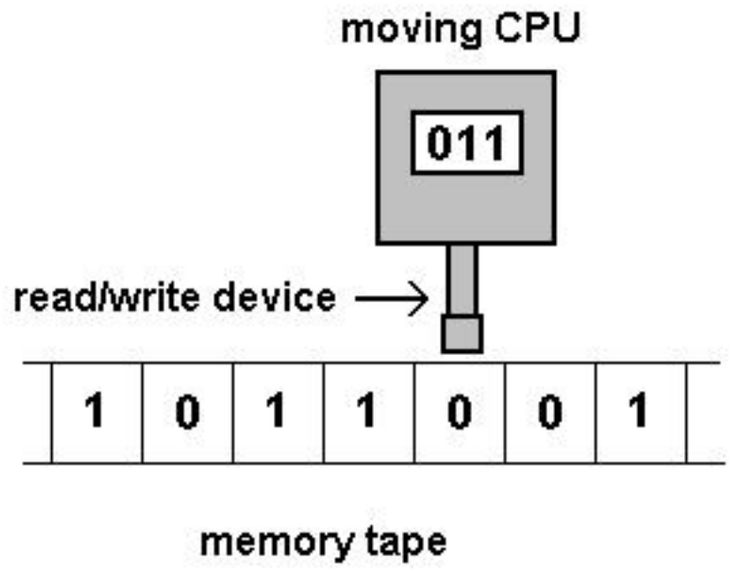

PSPACE problems
NP problems
NP complete
BQP
P problems


Semiconductor Devices


moving CPU
011
read/write device
1 0 1 1 0 0 1
memory tape


PROGRAMMING
CODING
CODE
PROGRAM
COMPUTER
SOURCE
SYSTEM
READABILITY
HARDWARE
INCLUDING
ALGORITHM
RESOURCES
OPERATING
DIFFERENT
PURPOSE
MEMORY
EASE
USER
MAKE
LANGUAGE
IMPLEMENTATION
PROBLEMS

Turing Machine



Quantum Turing Machine ?

Quantum theory, the Church-Turing principle and the universal quantum computer

DAVID DEUTSCH*

Appeared in *Proceedings of the Royal Society of London A* **400**, pp. 97-117 (1985)†

(*Communicated by R. Penrose, F.R.S. — Received 13 July 1984*)

2 Quantum computers

Every existing general model of computation is effectively classical. That is, a full specification of its state at any instant is equivalent to the specification of a set of numbers, all of which are in principle measurable. Yet according to quantum theory there exist no physical systems with this property. The fact that classical physics and the classical universal Turing machine do not obey the Church-Turing principle in the strong physical form (1.2) is one motivation for seeking a truly quantum model. The more urgent motivation is, of course, that classical physics is false.

Benioff (1982) has constructed a model for computation within quantum kinematics and dynamics, but it is still effectively classical in the above sense. It is constructed so that at the end of each elementary computational step, no characteristically quantum property of the model —interference, non-separability, or indeterminism — can be detected. Its computations can be perfectly simulated by a Turing machine.

Feynman (1982) went one step closer to a true quantum computer with his 'universal quantum simulator'. This consists of a lattice of spin systems with nearest-neighbour interactions that are freely specifiable. Although it can surely simulate any system with a finite-dimensional state space (I do not understand why Feynman doubts that it can simulate fermion systems), it is not a computing machine in the sense of this article. 'Programming' the simulator consists of endowing it by *fiat* with

Albert (1983) has described a quantum mechanical measurement 'automaton' and has remarked that its properties on being set to measure itself have no analogue among classical automata. Albert's automata, though they are not general purpose computing machines, are true quantum computers, members of the general class that I shall study in this section.

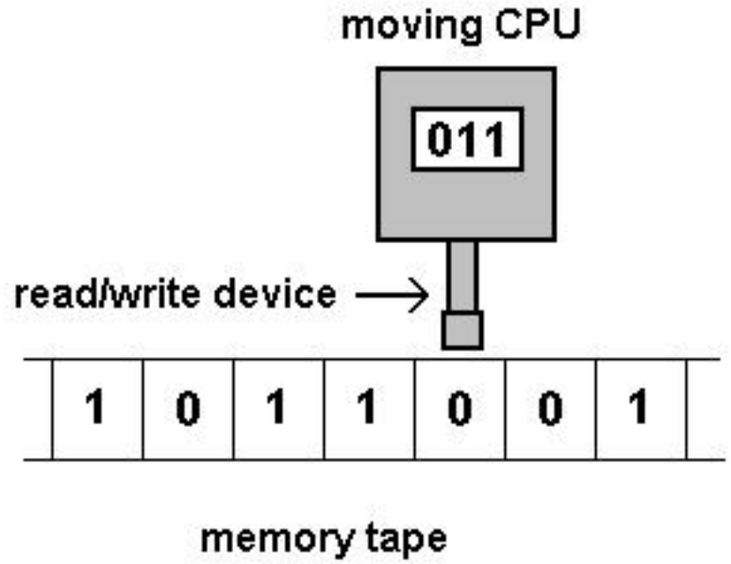
In this section I present a general, fully quantum model for computation. I then describe the universal quantum computer $\mathcal{Q}$, which is capable of perfectly simulating every finite, realizable physical system. It can simulate ideal closed (zero temperature) systems, including all other instances of quantum computers and quantum simulators, with arbitrarily high but not perfect accuracy. In computing strict functions from $\mathbb{Z}$ to $\mathbb{Z}$ it generates precisely the classical recursive functions $\mathrm{C}(\mathcal{T})$ (a manifestation of the correspondence principle). Unlike $\mathcal{T}$, it can simulate any finite classical discrete stochastic process perfectly. Furthermore, as we shall see in §3, it as many remarkable and potentially useful capabilities that have no classical analogues.

Like a Turing machine, a model quantum computer $\mathcal{Q}$, consists of two components, a finite processor and an infinite memory, of which only a finite portion is ever used. The computation proceeds in steps of fixed duration T, and during each step only the processor and a finite part of the memory interact, the rest of the memory remaining static.

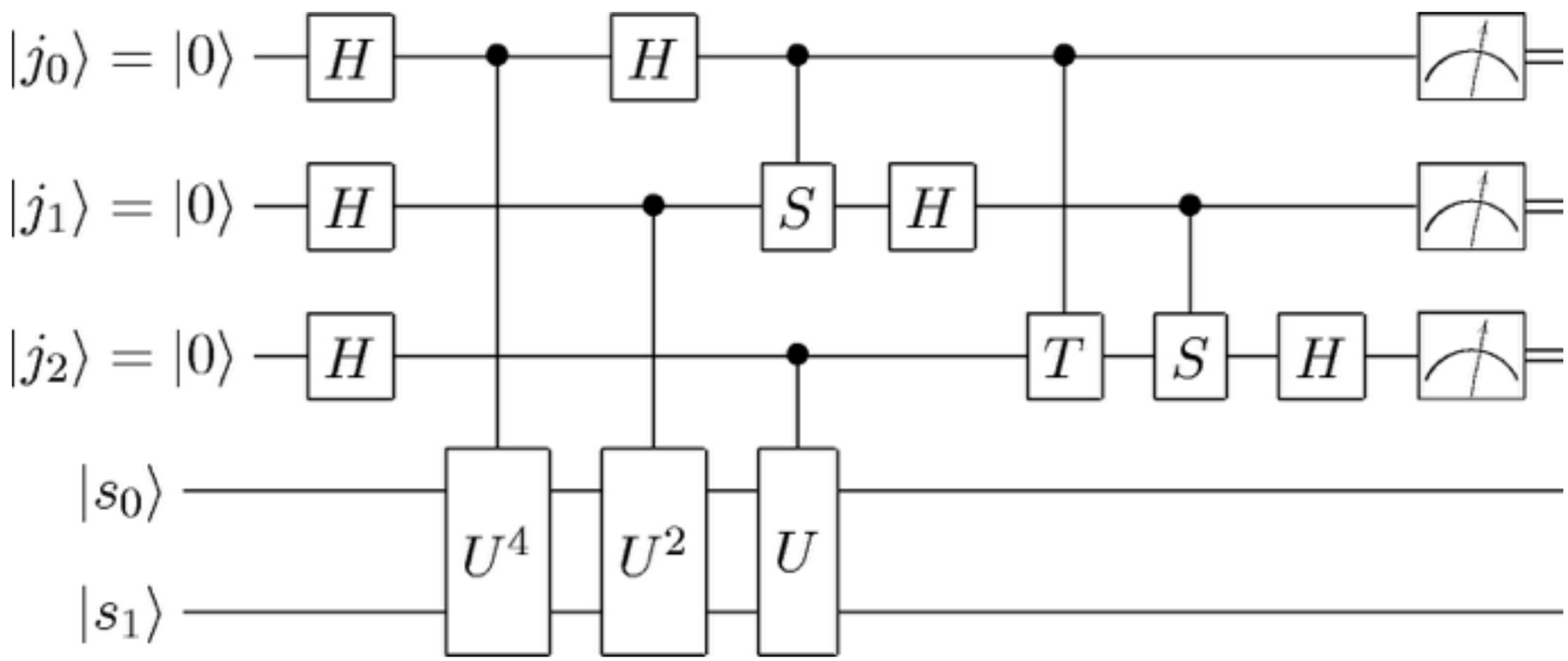
3 Properties of the universal quantum computer

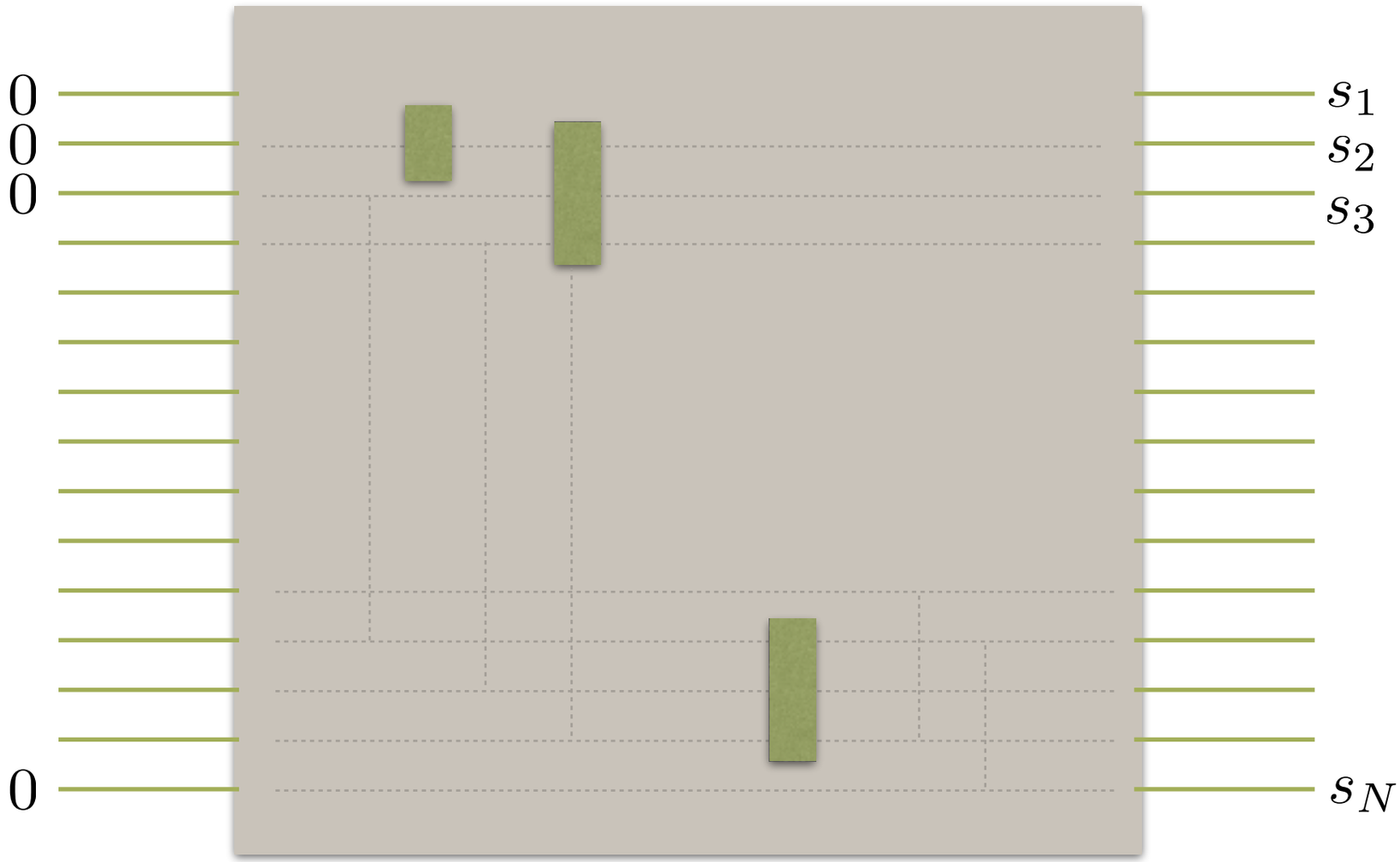
We have already seen that the universal quantum computer $\mathcal{Q}$ can perfectly simulate any Turing machine and can simulate with arbitrary precision any quantum computer or simulator. I shall now show how $\mathcal{Q}$ can simulate various physical systems, real and theoretical, which are beyond the scope of the universal Turing machine $\mathcal{T}$.

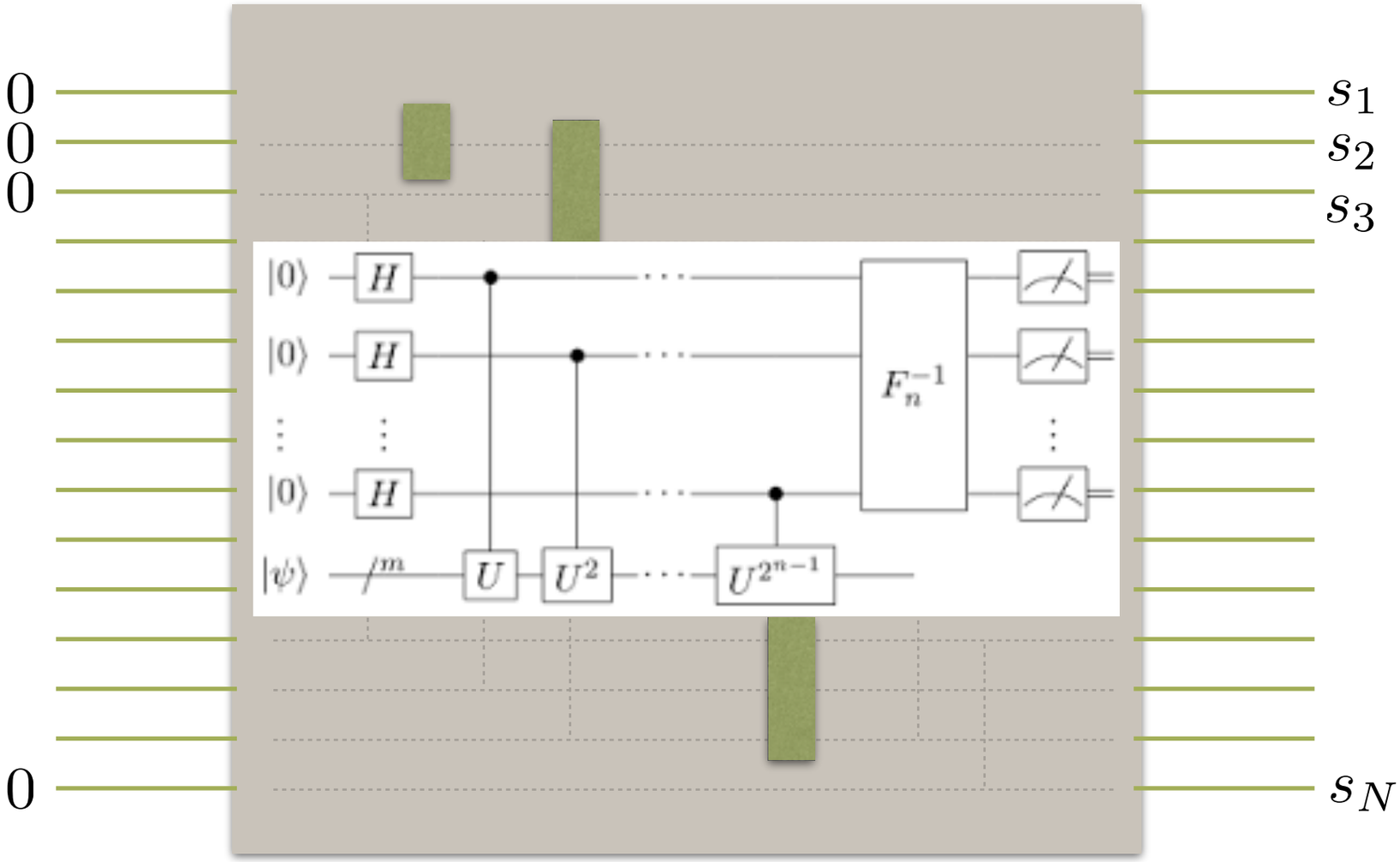
Turing Machine



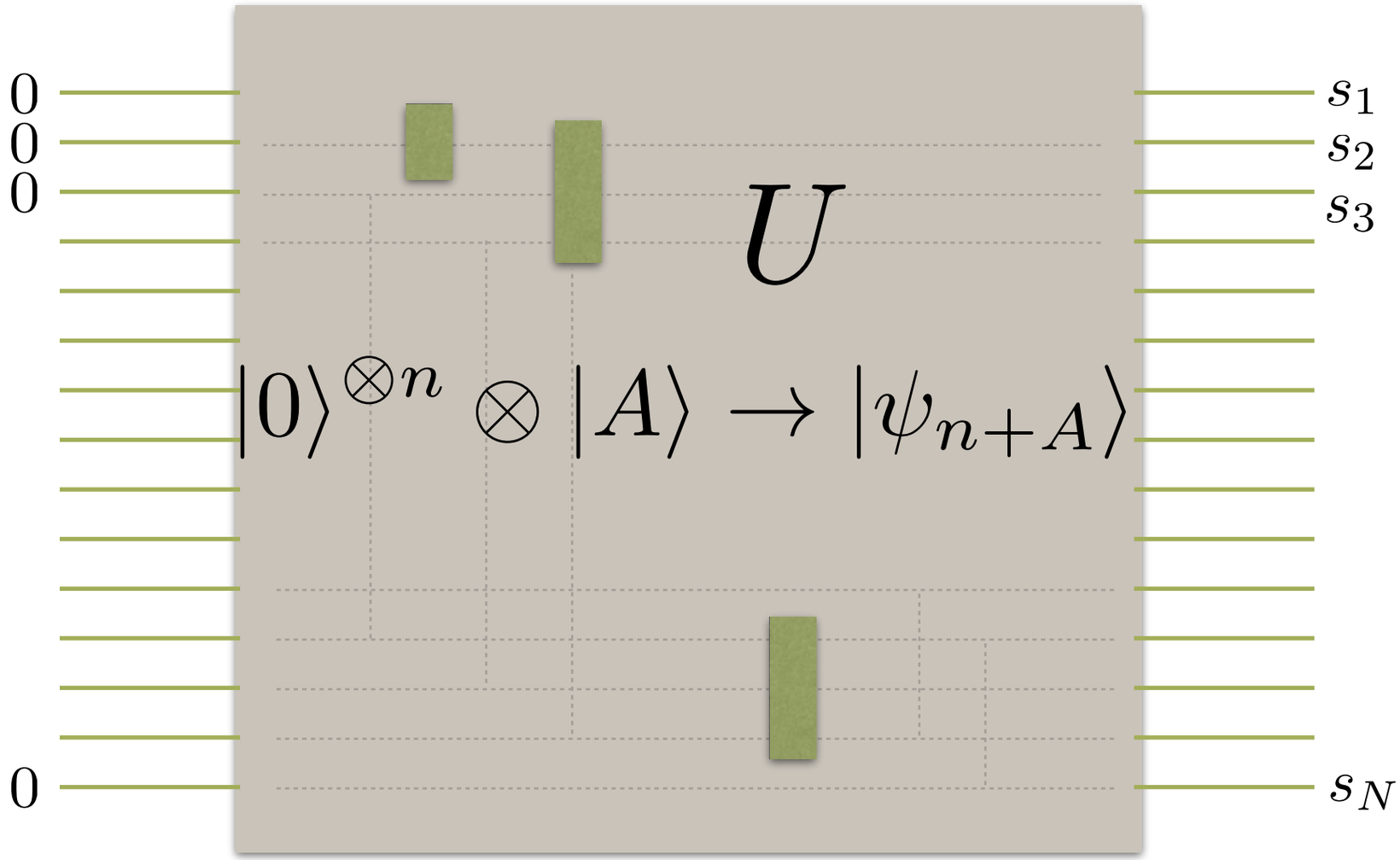
Quantum Turing Machine can be simulated in a quantum circuit




0
0
0
0
s_1
s_2
s_3
s_N


0
0
0
0
s_1
s_2
s_3
s_N
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|\psi\rangle$
H
H
H
$/^m$
U
U^2
$U^{2^{n-1}}$
F_n^{-1}

Quantum Computation: Exploit quantum dynamics for computational purposes



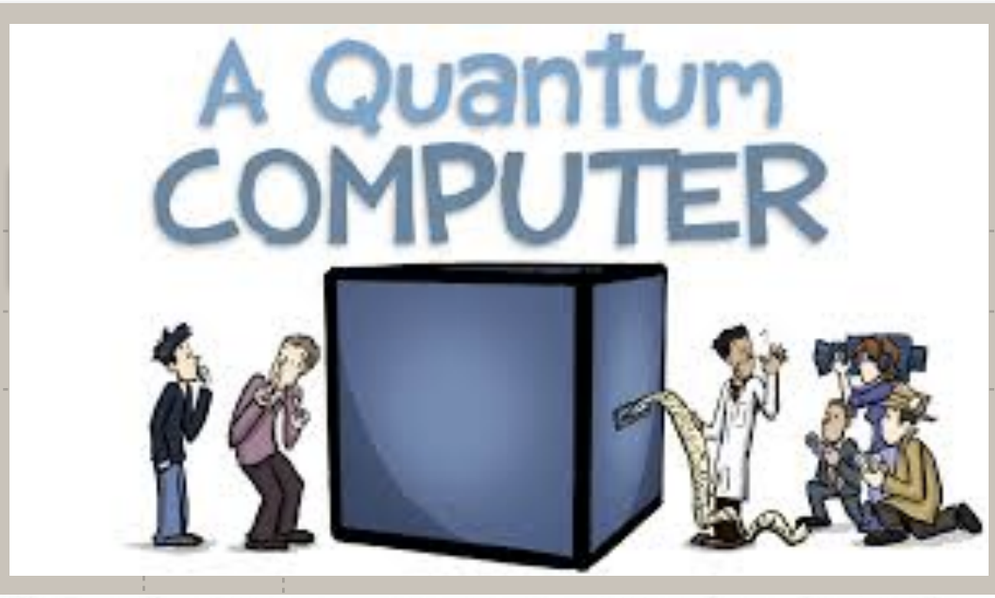
Solovay-Kitaev theorem $\forall U \quad \exists\{U_2,\ U_1\},\ \text{s. t.}\ \|U - \Pi_j(U_j)\| \leq \epsilon$

Products of Two- and single qubit unitary transformations can efficiently simulate arbitrary unitary transformations

universal set of gates : CNOT gate + single-qubit operations

0
0
0

s_1
s_2
s_3



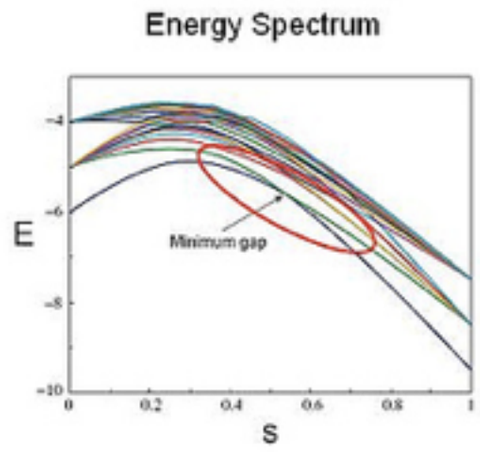
Adiabatic Quantum Computation (AQC)

E. Farhi et al., Science 292, 472 (2001)

System Hamiltonian:

$$H = (1-s)\,H_i + s\,H_f$$

Linear interpolation: $s = t/t_f$



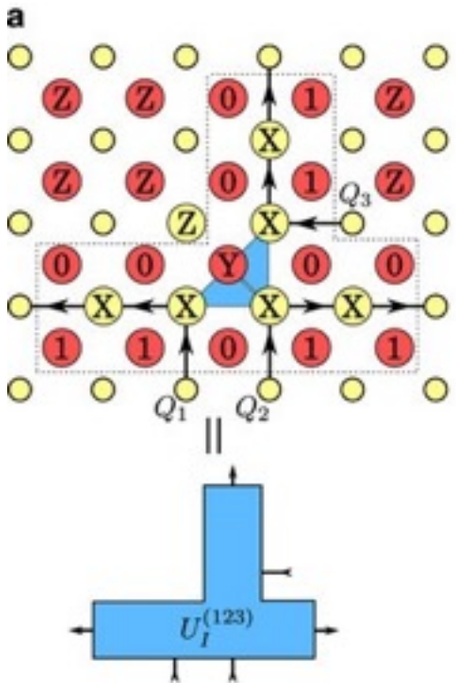
- Ground state of H_i is easily accessible.
- Ground state of H_f encodes the solution to a hard computational problem.

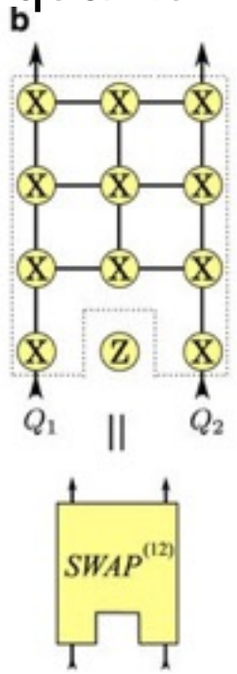
0

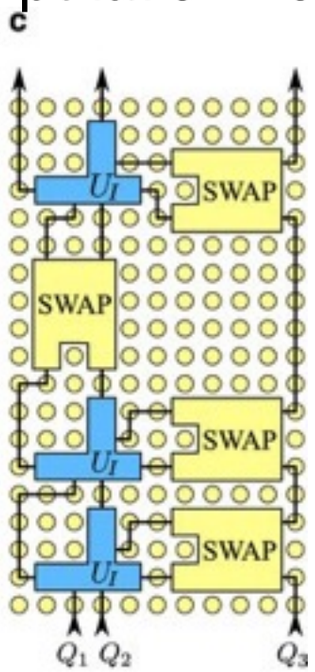
s_N

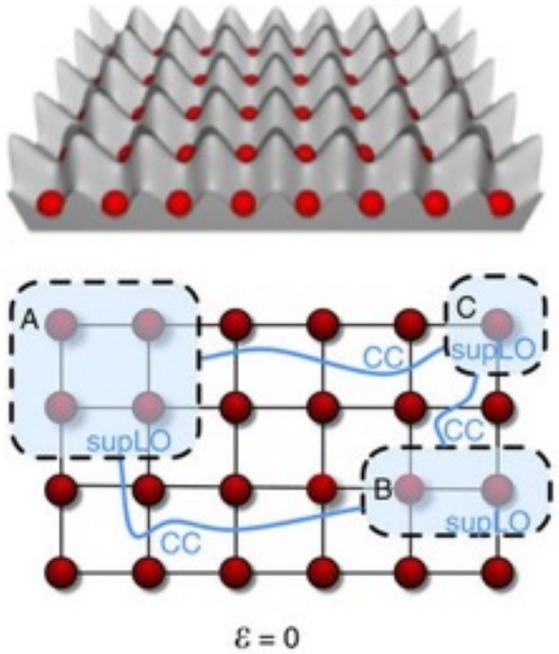
D. Aharonov *et. al.*, Adiabatic quantum computation is equivalent to standard quantum computation
Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS'04)

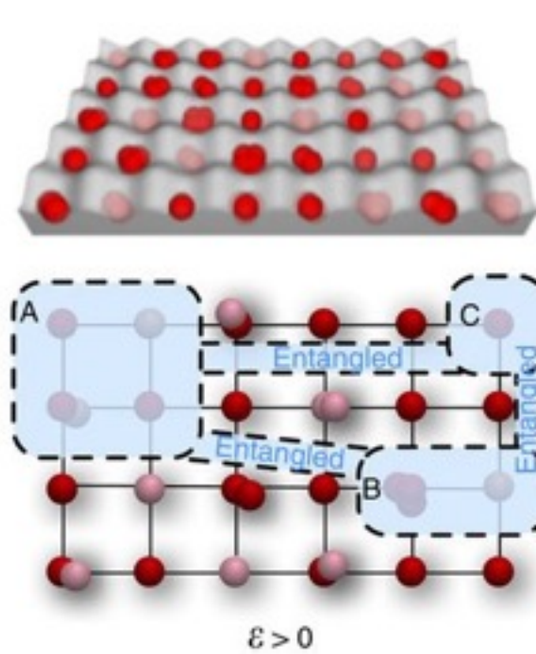
Measurement-based quantum computation : entanglement is the key resource

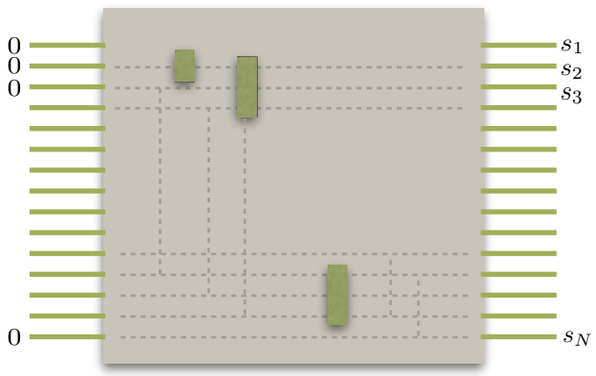


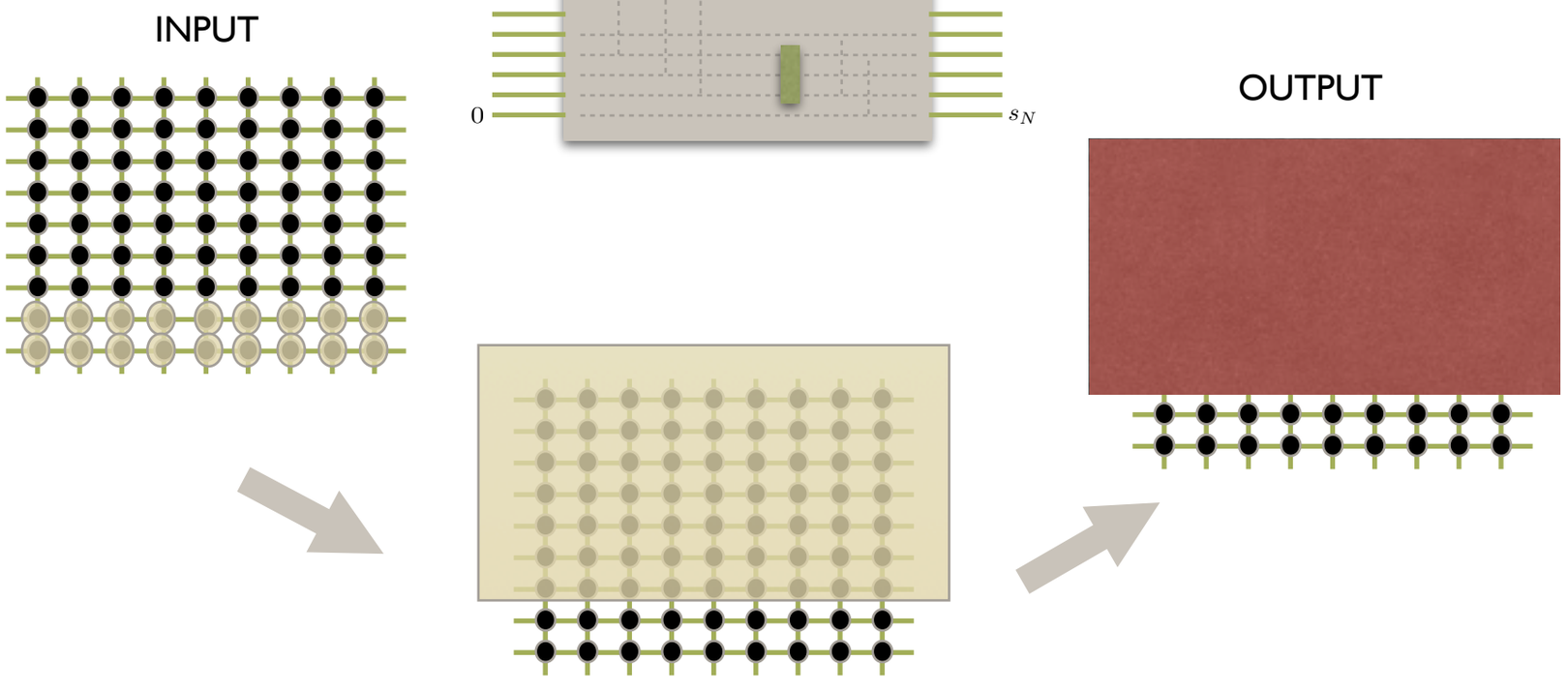




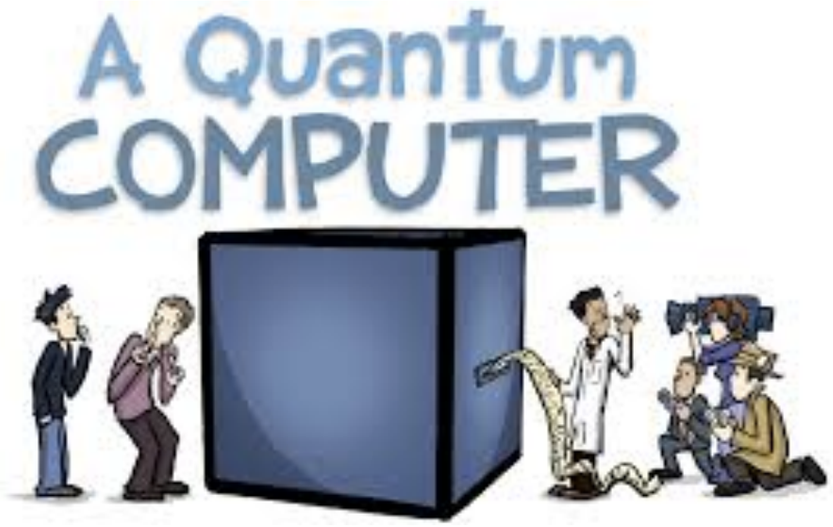


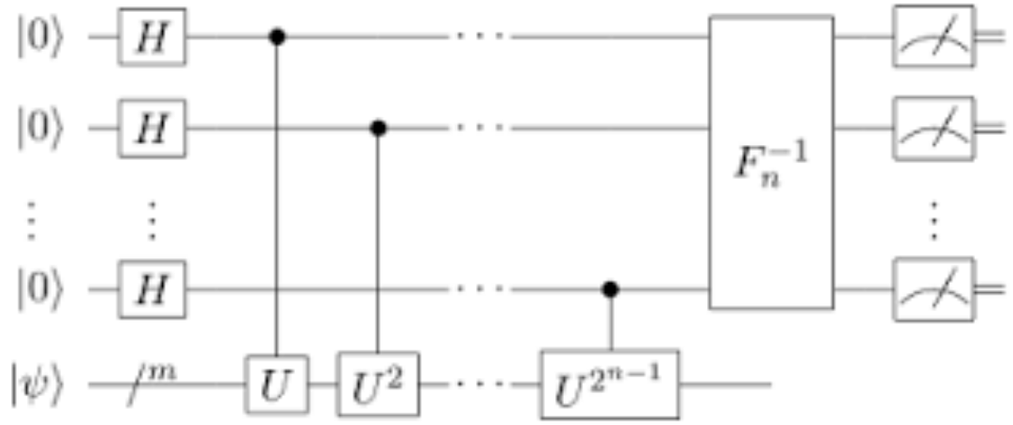


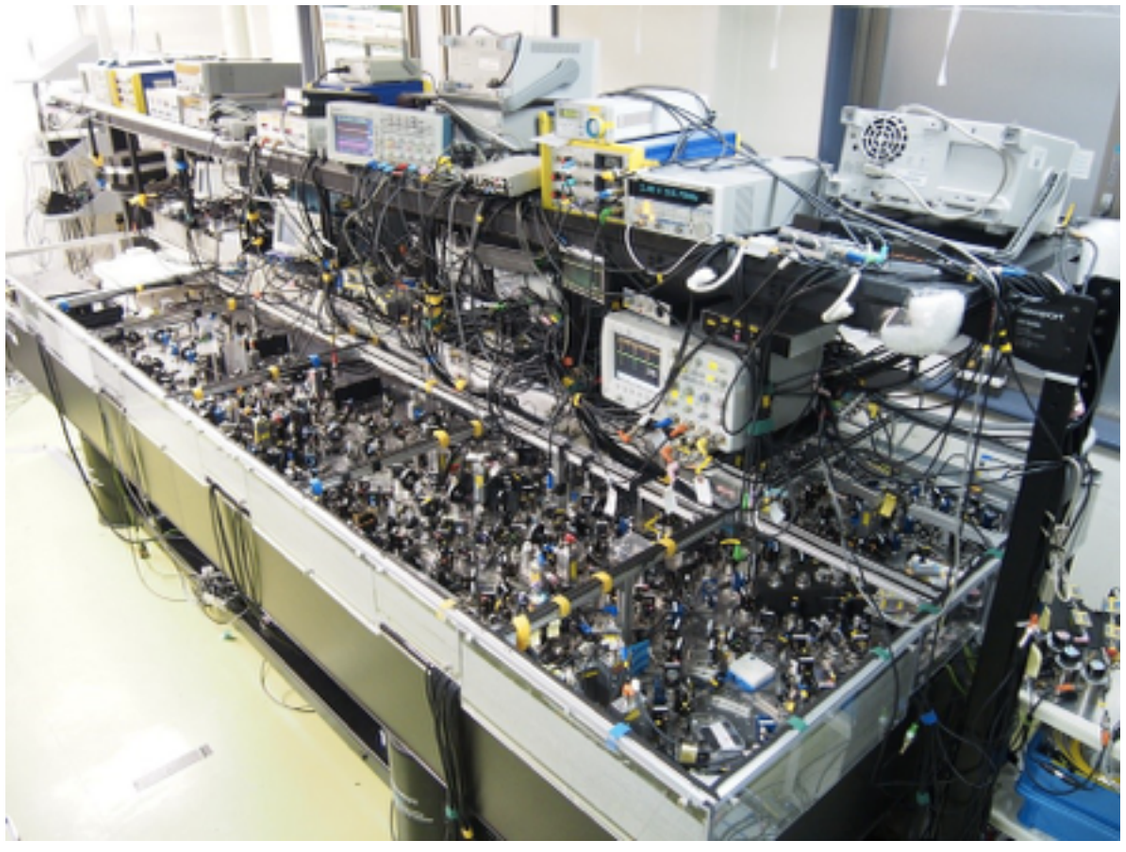


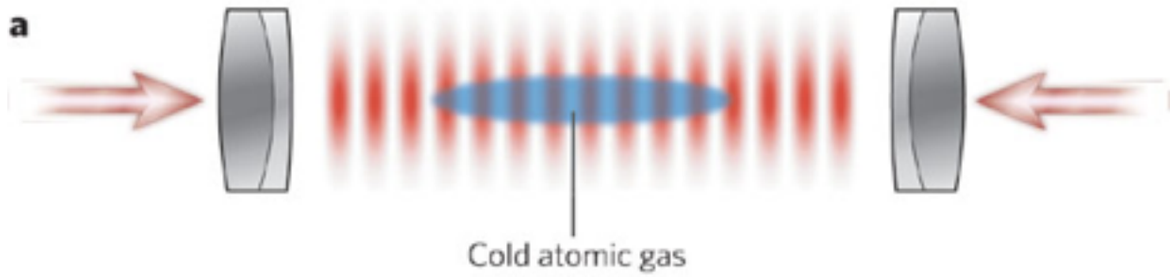


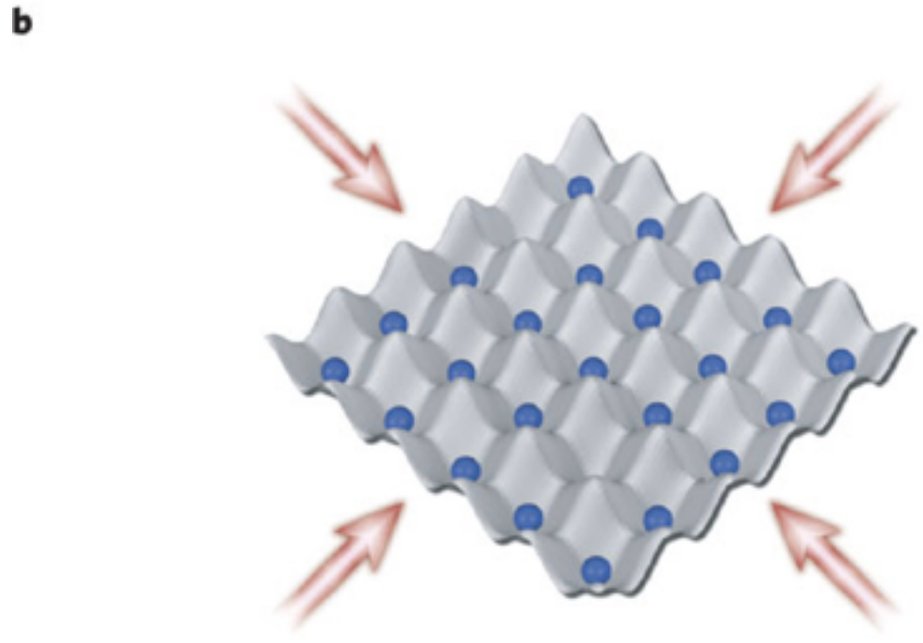
One-way quantum computer: R. Raussendorff and H. Briegel, PRL 2001
Figure. J. Miller and A. Miyake, npj QI 2016 ; M. Cramer et al. Nat. Comm. 2013


A Quantum
COMPUTER


$|0\rangle$
$|0\rangle$
$|0\rangle$
$|\psi\rangle$
H
H
H
m
U
U^2
$U^{2^{n-1}}$
F_n^{-1}



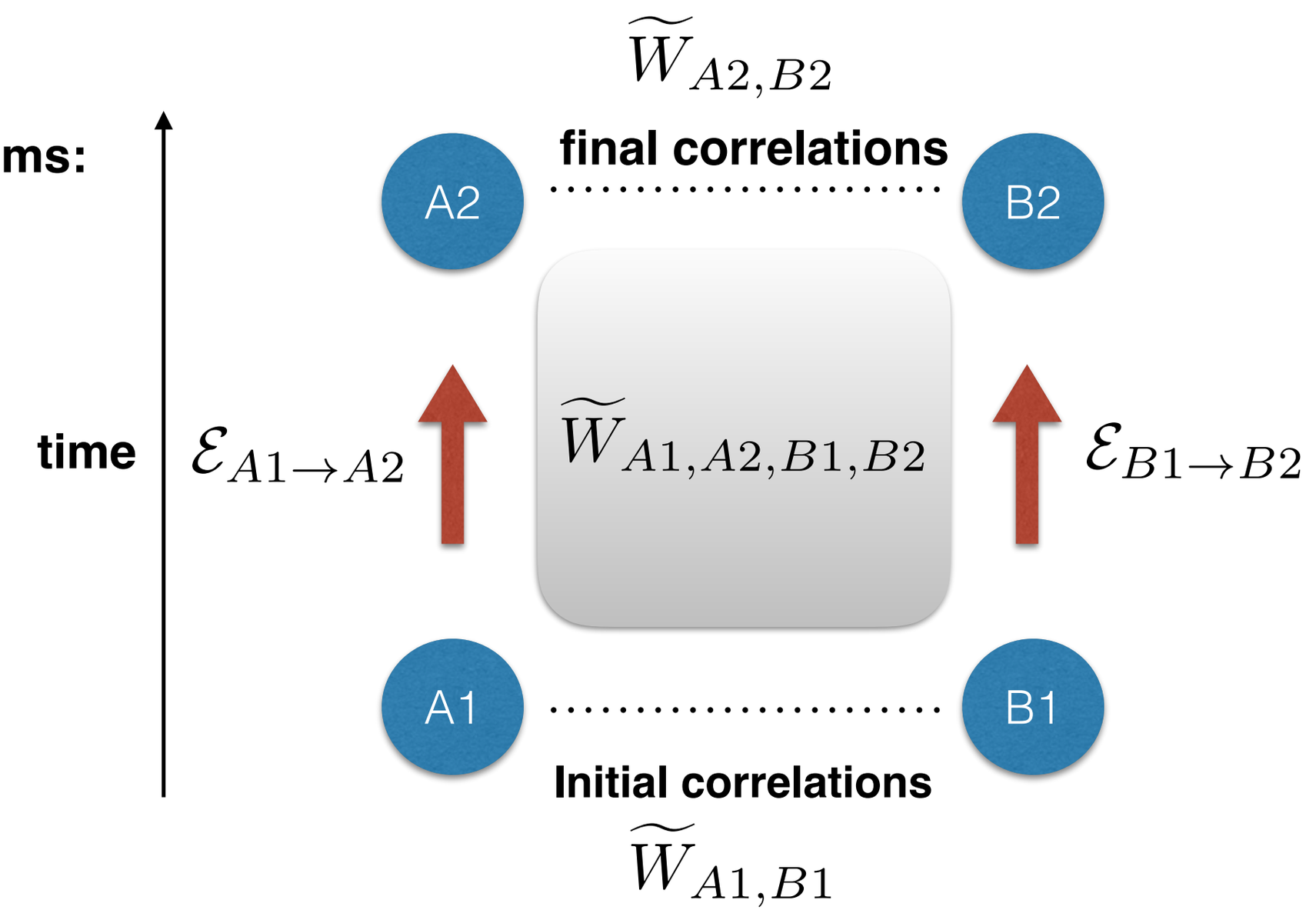

a
Cold atomic gas


b

Is quantum computer faster?

on-going efforts in the group of Joonwoo Bae

Causation in Quantum Systems:
Local Laboratories
(Well-defined local maps)

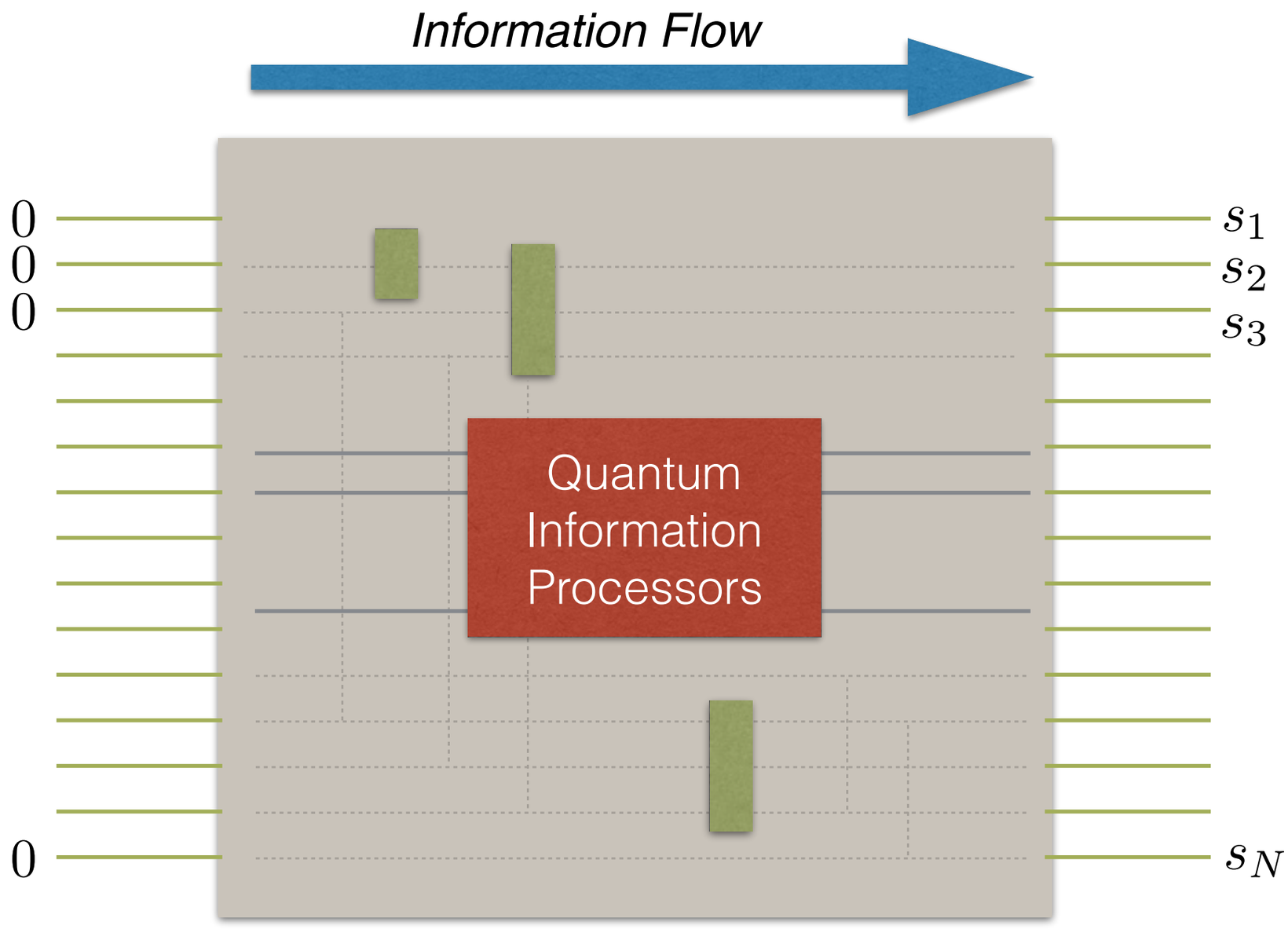


Main Question:

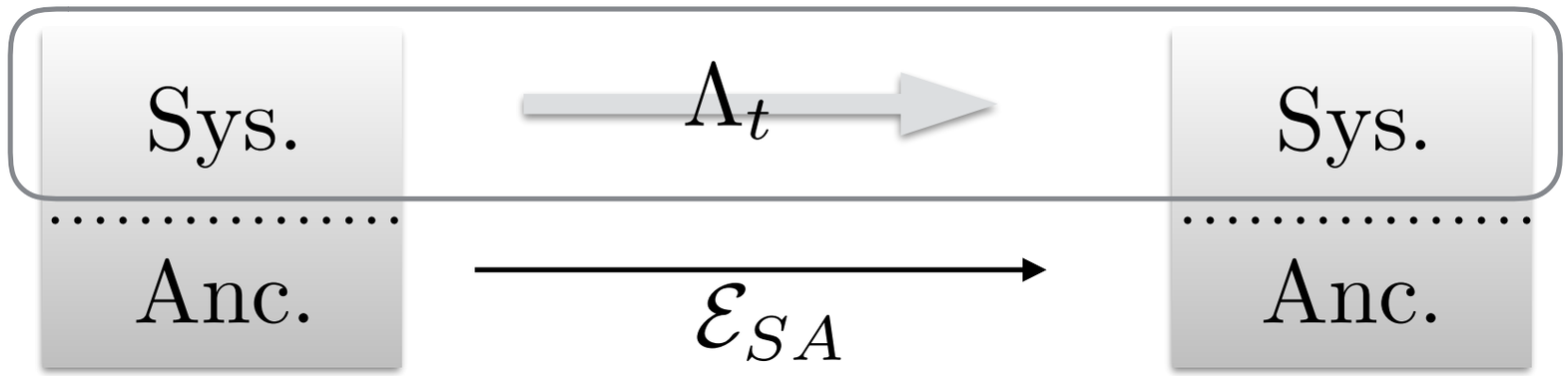
Problem 1. What's the causation from the approximately symmetric subspace?
(in the picture of Reichenbach common cause principle)

Applications: Causal Quantum Networks, Channel Capacities of Causal Networks

(fundamental) Analysis of *Information Flow* - the origin of the computational power



	Quantum Information Theory	Classical Information Theory
State	$\rho \in S(\mathcal{H})$	$p(x)$
Dynamics	Completely positive maps $I \otimes \Lambda \geq 0$	Positive maps (stochastic process) $\Lambda \geq 0$
Dynamical Maps	$\frac{d}{dt}\rho(t) = \mathcal{L}_t \rho(t)$	$p(x_n, t_n; x_{n-1}, t_{n-1}; \cdots ; x_0, t_0)$ $= \prod_{i=1}^{n} p(x_i, t_i \vert x_{i-1}, t_{i-1}) p(x_0, t_0)$



Colloquium: Non-Markovian dynamics in open quantum systems

Heinz-Peter Breuer*

Physikalisches Institut, Universität Freiburg, Hermann-Herder-Straße 3, D-79104 Freiburg, Germany

Elsi-Mari Laine

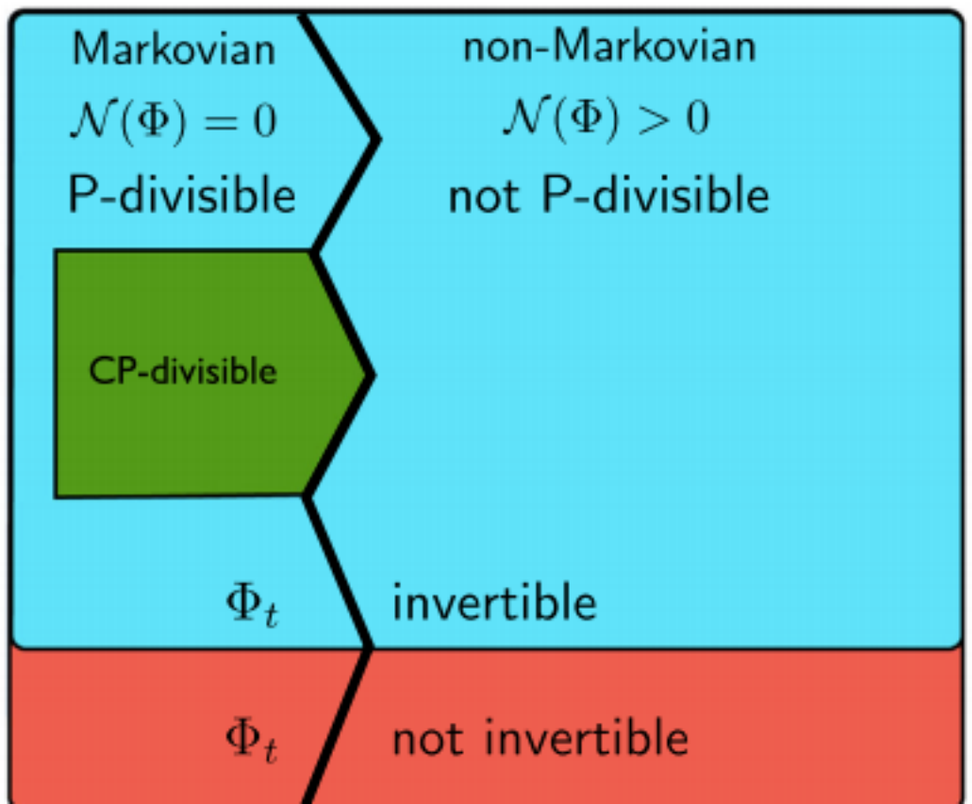
QCD Labs, COMP Centre of Excellence, Department of Applied Physics, Aalto University, P.O. Box 13500, FI-00076 AALTO, Finland and Turku Centre for Quantum Physics, Department of Physics and Astronomy, University of Turku, FI-20014 Turun yliopisto, Finland

Jyrki Piilo

Turku Centre for Quantum Physics, Department of Physics and Astronomy, University of Turku, FI-20014 Turun yliopisto, Finland

Bassano Vacchini

Dipartimento di Fisica, Università degli Studi di Milano, Via Celoria 16, I-20133 Milan, Italy and INFN, Sezione di Milano, Via Celoria 16, I-20133 Milan, Italy



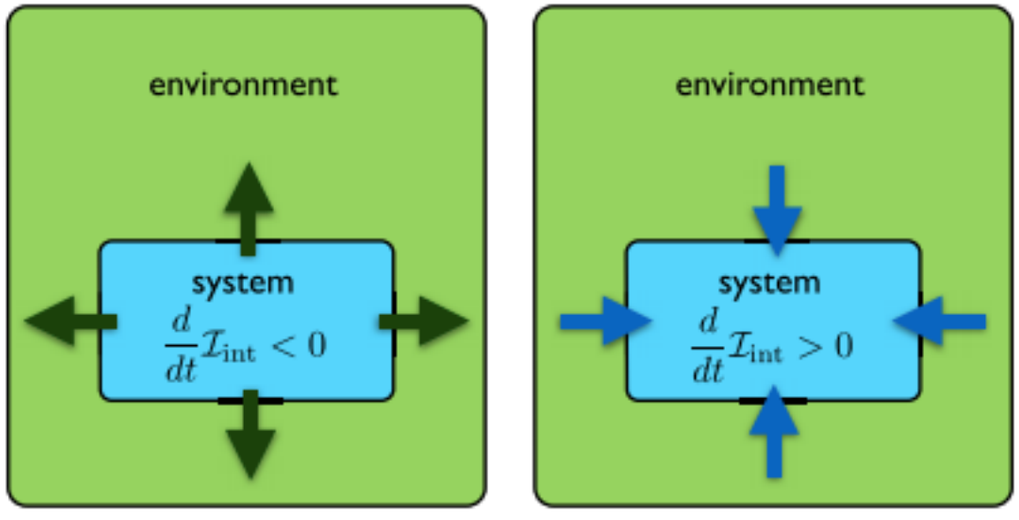


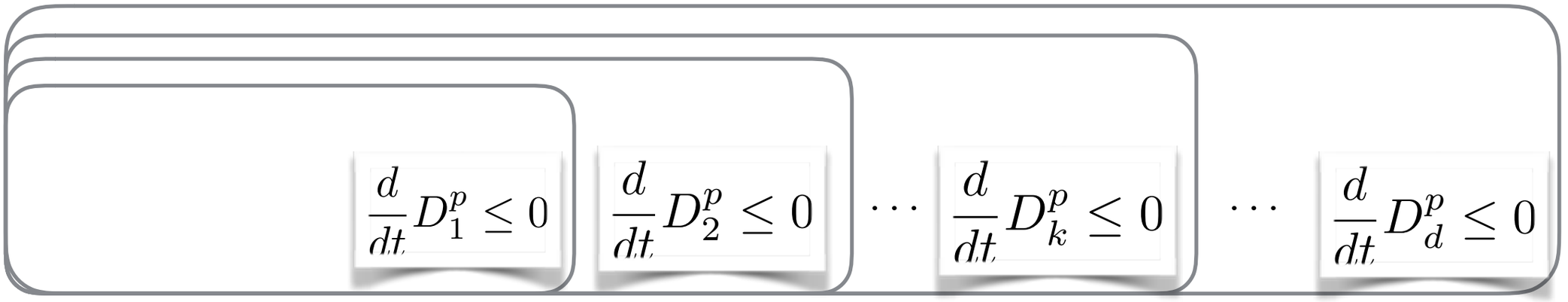
FIG. 3. The information flow between an open system and its environment according to Eq. (32). Left: The open system loses information to the environment, corresponding to a decrease of $\mathcal{I}_{\rm int}(t)$ and Markovian dynamics. Right: Non-Markovian dynamics is characterized by a backflow of information from the environment to the system and a corresponding increase of $\mathcal{I}_{\rm int}(t)$.

$$\sigma(t) \equiv \frac{d}{dt} D(\Phi_t \rho_S^1, \Phi_t \rho_S^2)$$

Operational characterization of k-divisiblity

Main result. Λ_t is k-divisible iff $p \in [0,1]$ $\forall \Phi_1, \Phi_2$ CP maps, $\frac{d}{dt} D_k^p(\Lambda_t \circ \Phi_1, \Lambda_t \circ \Phi_2) \leq 0$

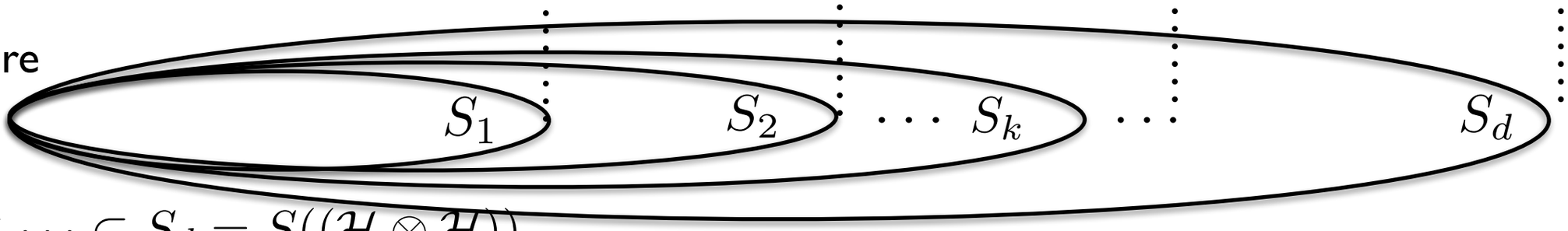
k-divisiblity



Operational measure*
The more entangled, the more useful!

$$D_1^p[\Phi_1, \Phi_2] < D_2^p[\Phi_1, \Phi_2] < \cdots < D_k^p[\Phi_1, \Phi_2] < \quad < D_d^p[\Phi_1, \Phi_2]$$

Entanglement structure



$$S_{\text{sep}} = S_1 \subset S_2 \subset \cdots \subset S_d = S((\mathcal{H} \otimes \mathcal{H}))$$

PRL 117, 050403 (2016) PHYSICAL REVIEW LETTERS week ending 29 JULY 2016

Operational Characterization of Divisibility of Dynamical Maps

Joonwoo Bae[1,2] and Dariusz Chruściński[3]
[1]*Department of Applied Mathematics, Hanyang University (ERICA), 55 Hanyangdaehak-ro, Ansan, Gyeonggi-do 426-791, Korea*
[2]*Freiburg Institute for Advanced Studies (FRIAS), Albert-Ludwigs University of Freiburg, Albertstrasse 19, 79104 Freiburg, Germany*
[3]*Institute of Physics, Faculty of Physics, Astronomy, and Informatics, Nicolaus Copernicus University,*

Information-theoretic characterization of k-divisiblity

Main result. Λ_t is k-divisible iff $p \in [0,1]$ $\forall \Phi_1, \Phi_2$ CP maps, $\frac{d}{dt} D_k^p(\Lambda_t \circ \Phi_1, \Lambda_t \circ \Phi_2) \leq 0$

$$D_k^p(\Lambda_t \circ \Phi_1, \Lambda_t \circ \Phi_2) = \max_{\rho \in S_k} \|p[\mathrm{id} \otimes \Lambda_t \circ \Phi_1](\rho) - (1-p)[\mathrm{id} \otimes \Lambda_t \circ \Phi_2](\rho)\|_1$$

$$S_k = \{\rho \in S(\mathcal{H} \otimes \mathcal{H}) : SN(\rho) \leq k,\ SN(\rho) = \min_{p_j, \psi_j} (\max_j SR(\psi_j))\}$$

Main result.' Λ_t is k-divisible iff $p \in [0,1]$ $\forall \Phi_1, \Phi_2$ CP maps, $\frac{d}{dt} H_{\min}(A|B)_{\rho_{AB_k}(t)} \geq 0$

$$\rho_{AB_k}(t) = \sum_{i=1,2} q_i |i\rangle\langle i|_A \otimes (\mathrm{id}_k \otimes \Lambda_t \circ \Phi_i)[\rho]_B$$

PRL 117, 050403 (2016) PHYSICAL REVIEW LETTERS week ending 29 JULY 2016

Operational Characterization of Divisibility of Dynamical Maps

Joonwoo Bae[1,2] and Dariusz Chruściński[3]
[1]*Department of Applied Mathematics, Hanyang University (ERICA), 55 Hanyangdaehak-ro, Ansan, Gyeonggi-do 426-791, Korea*
[2]*Freiburg Institute for Advanced Studies (FRIAS), Albert-Ludwigs University of Freiburg, Albertstrasse 19, 79104 Freiburg, Germany*
[3]*Institute of Physics, Faculty of Physics, Astronomy, and Informatics, Nicolaus Copernicus University, Grudziadzka 5, 87-100 Torun, Poland*
(Received 29 February 2016; published 27 July 2016)

In this work, we show the operational characterization to the divisibility of dynamical maps in terms of the distinguishability of quantum channels. It is proven that the distinguishability of any pair of quantum channels does not increase under divisible maps, in which the full hierarchy of divisibility is isomorphic to

Quantum Evolution ~ Resource Theories ~ Quantum Computation ~ …

- Applications: Detection Methods of Correlations, via the Operational Characterisation
- Inf. Theory: Min-entropy versus Conditional Mutual Information, in Markovian or k-divisible Dynamics
- Resource theory: Entanglement and Non-Markovianity
- Thermodynamics vs k-divisibility
- (semi-) Device-Independent Quantum Information Processing*

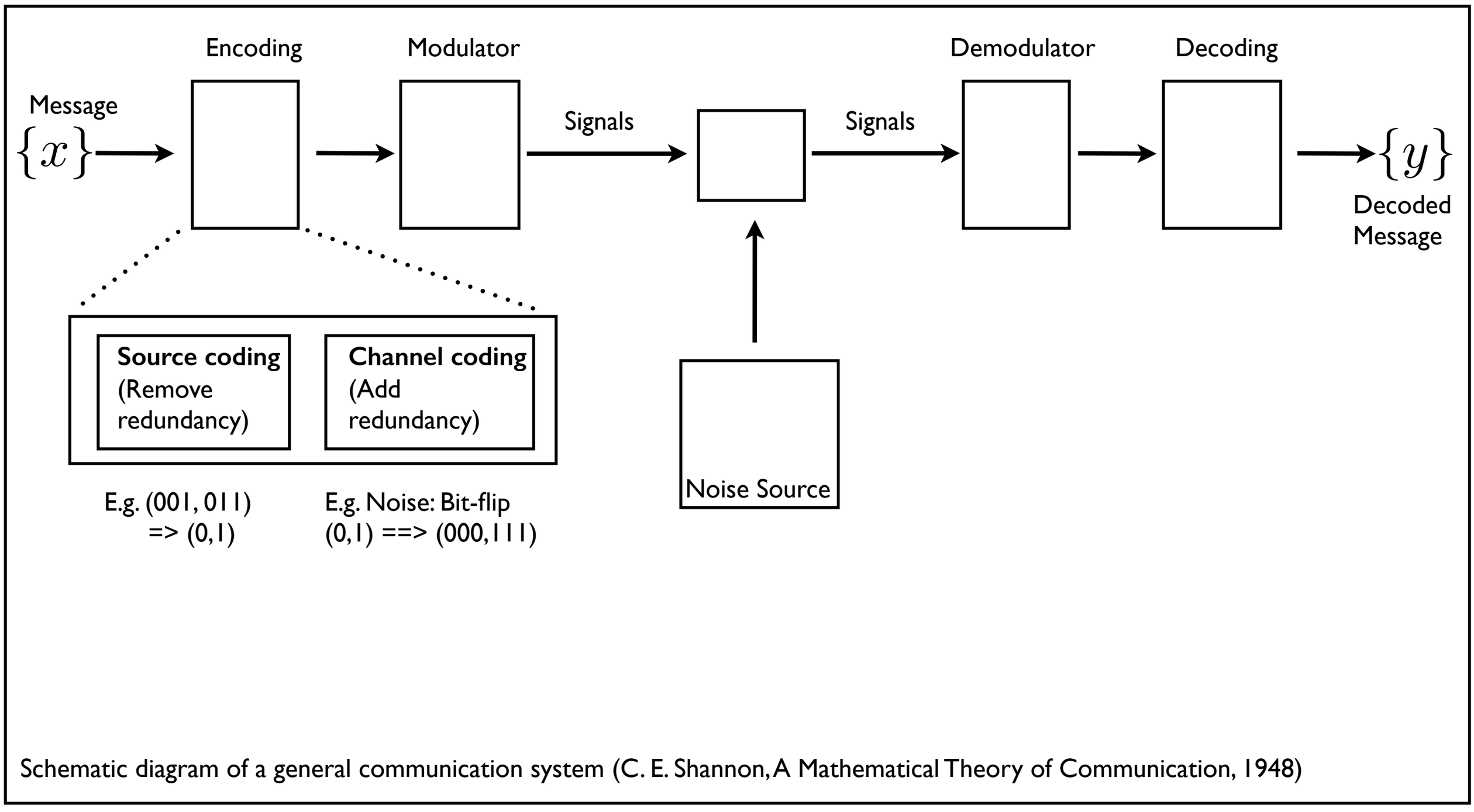
*No-signaling principle can tightly characterise the guessing probability, trace-norm (cb norms)

- Properties of Maps Induced from Entanglement Structure**

. . . . . .

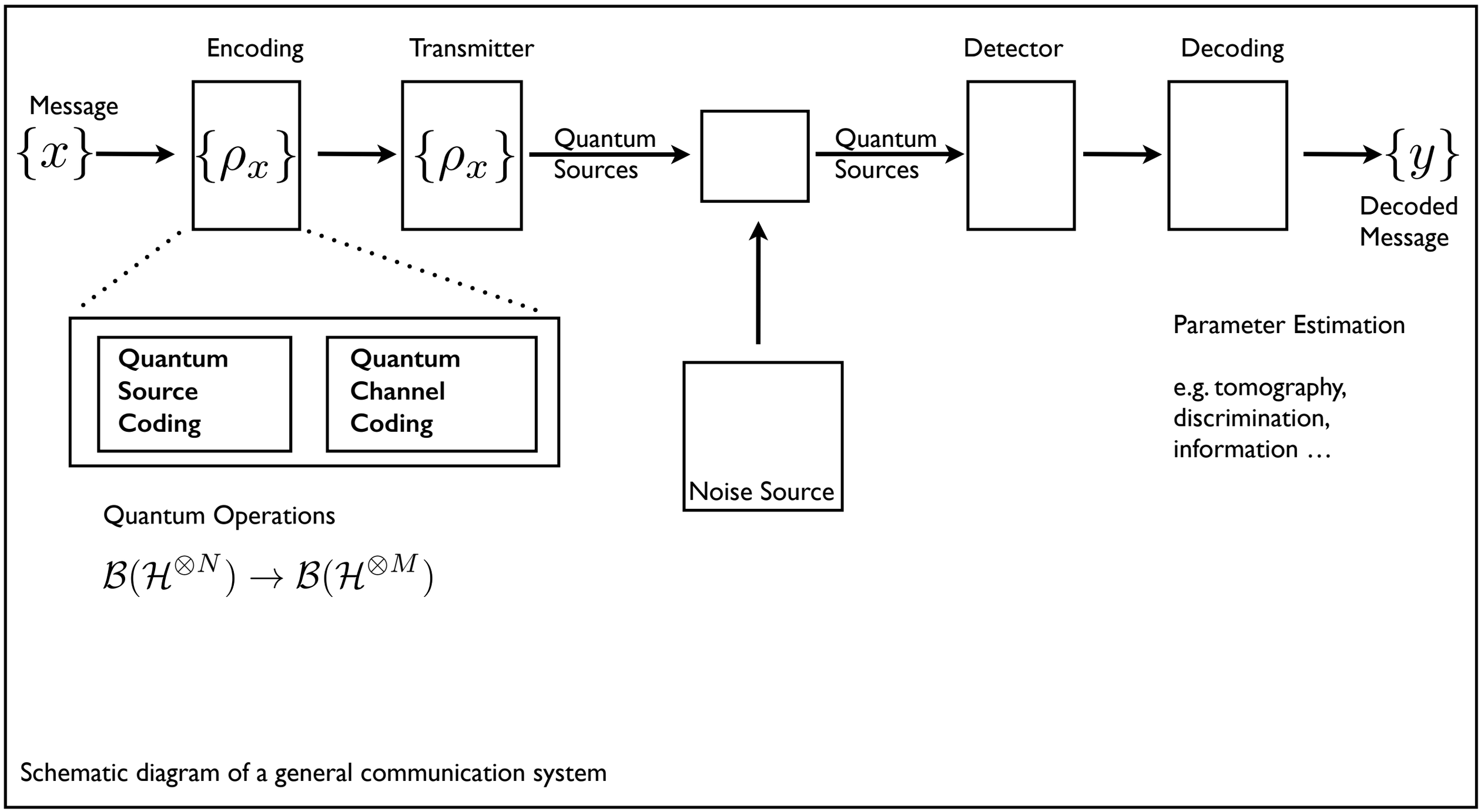
Quantum Information Theory

Communication-centric view



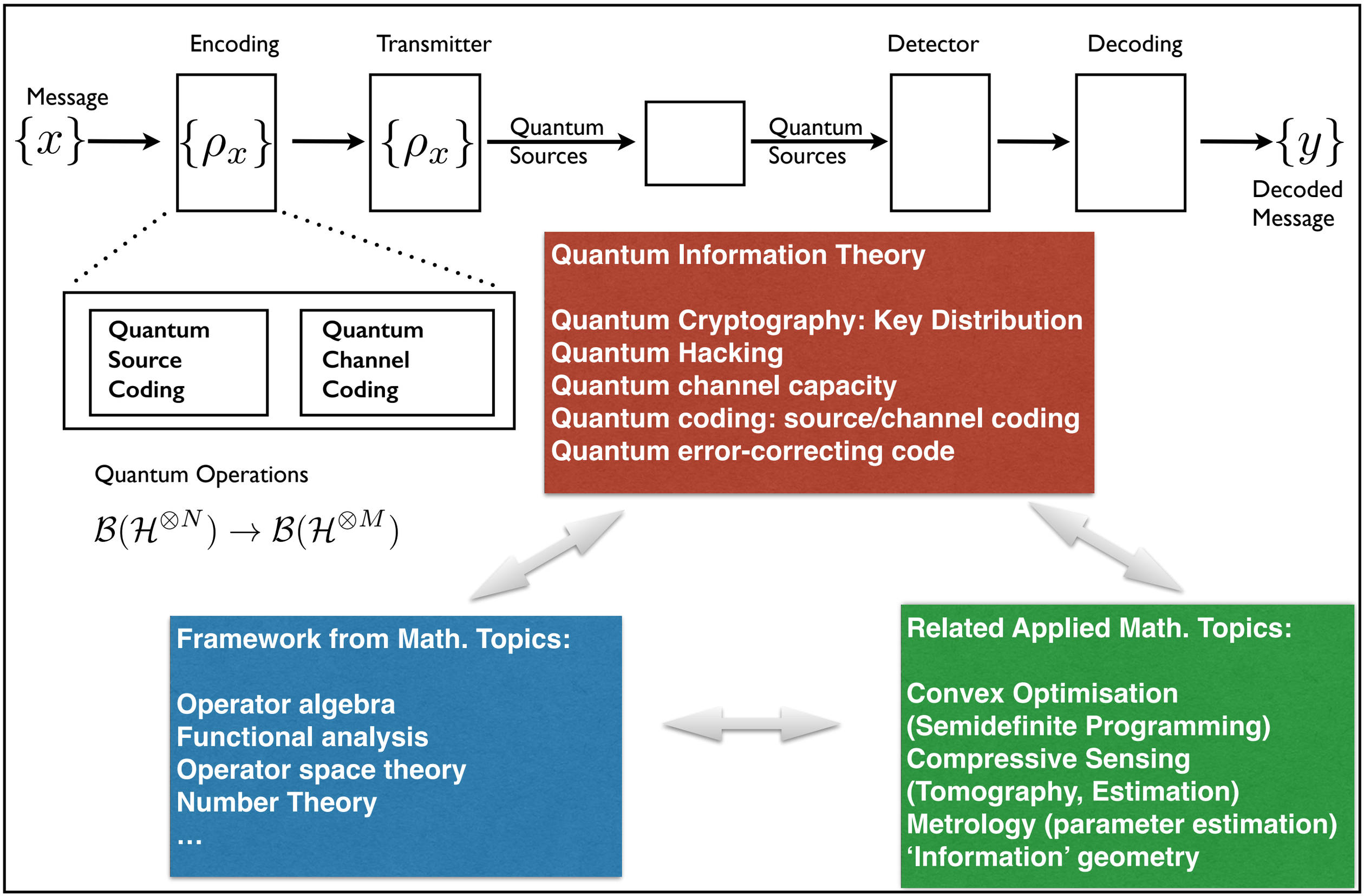
Schematic diagram of a general communication system (C. E. Shannon, A Mathematical Theory of Communication, 1948)

Communication-centric view

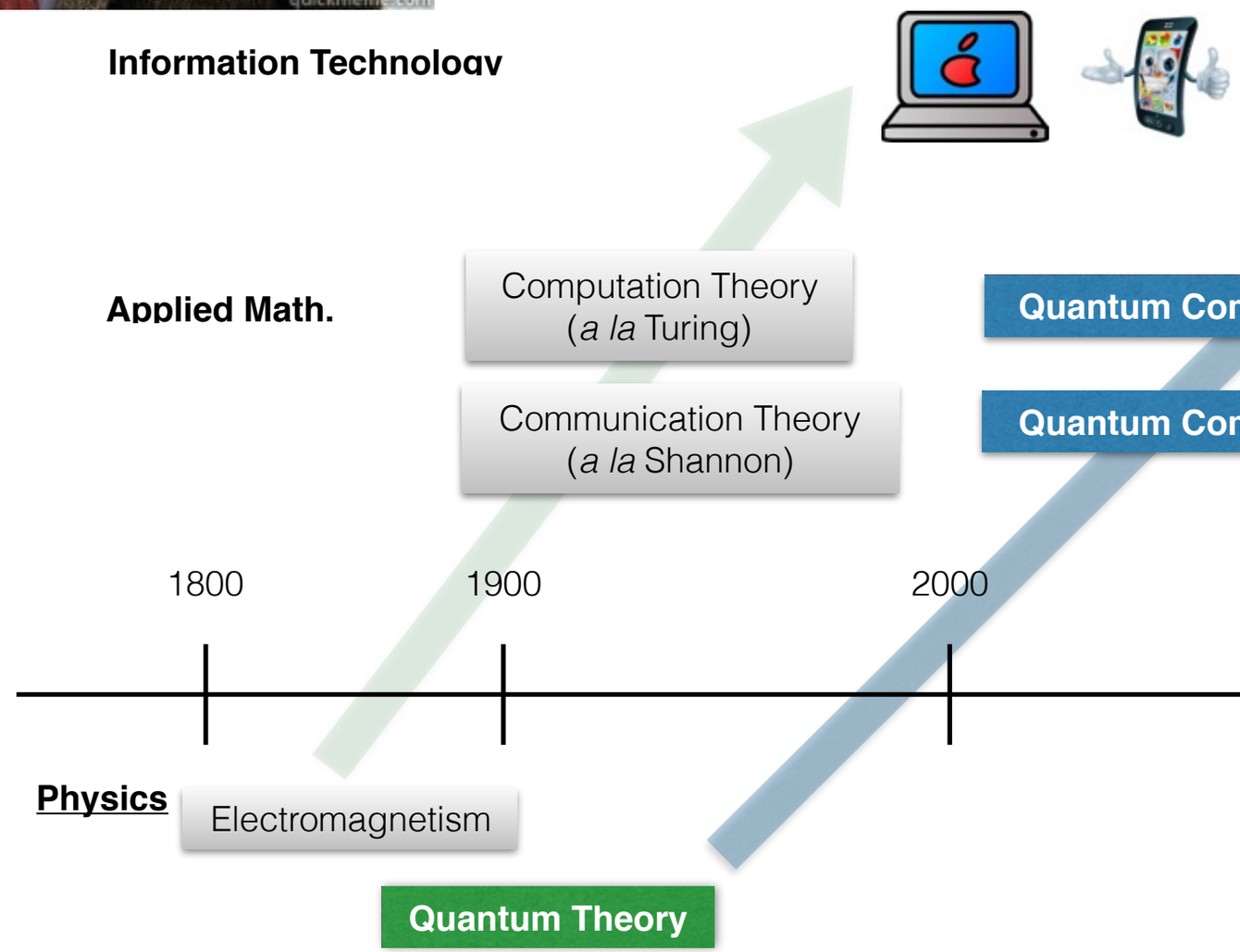


Schematic diagram of a general communication system

Communication-centric view




thank you for attention
any
questions ??????
quickmeme.com


Information Technology
Quantum IT?
Applied Math.
Computation Theory
(a la Turing)
Communication Theory
(a la Shannon)
Quantum Computation
Quantum Communication
1800
1900
2000
Physics
Electromagnetism
Quantum Theory

IOP Publishing

Reports on Progress in Physics

Rep. Prog. Phys. **80** (2017) 104001 (26pp)

https://doi.org/10.1088/1361-6633/aa7d45

Report on Progress

Designing quantum information processing via structural physical approximation

Joonwoo Bae

Department of Applied Mathematics, Hanyang University (ERICA), 55 Hanyangdaehak-ro, Ansan, Gyeonggi-do, 426-791, Republic of Korea
Freiburg Institute for Advanced Studies (FRIAS), Albert-Ludwigs University of Freiburg, Albertstrasse 19, 79104 Freiburg, Germany

E-mail: bae.joonwoo@gmail.com and joonwoobae@hanyang.ac.kr

Received 31 January 2017
Accepted for publication 3 July 2017
Published 14 September 2017

Corresponding Editor Professor Maciej Lewenstein

Abstract

In quantum information processing it may be possible to have efficient computation and secure communication beyond the limitations of classical systems. In a fundamental point of view, however, evolution of quantum systems by the laws of quantum mechanics is more restrictive than classical systems, identified to a specific form of dynamics, that is, unitary transformations and, consequently, positive and completely positive maps to subsystems. This also characterizes classes of disallowed transformations on quantum systems, among which positive but not completely maps are of particular interest as they characterize entangled states, a general resource in quantum information processing. Structural physical approximation offers a systematic way of approximating those non-physical maps, positive but not completely positive maps, with quantum channels. Since it has been proposed as a method of detecting entangled states, it has stimulated fundamental problems on classifications of positive maps and the structure of Hermitian operators and quantum states, as well as