Can QKD Counter The Threat Posed by Quantum Computers To Public Key Encryption

Alan Woodward

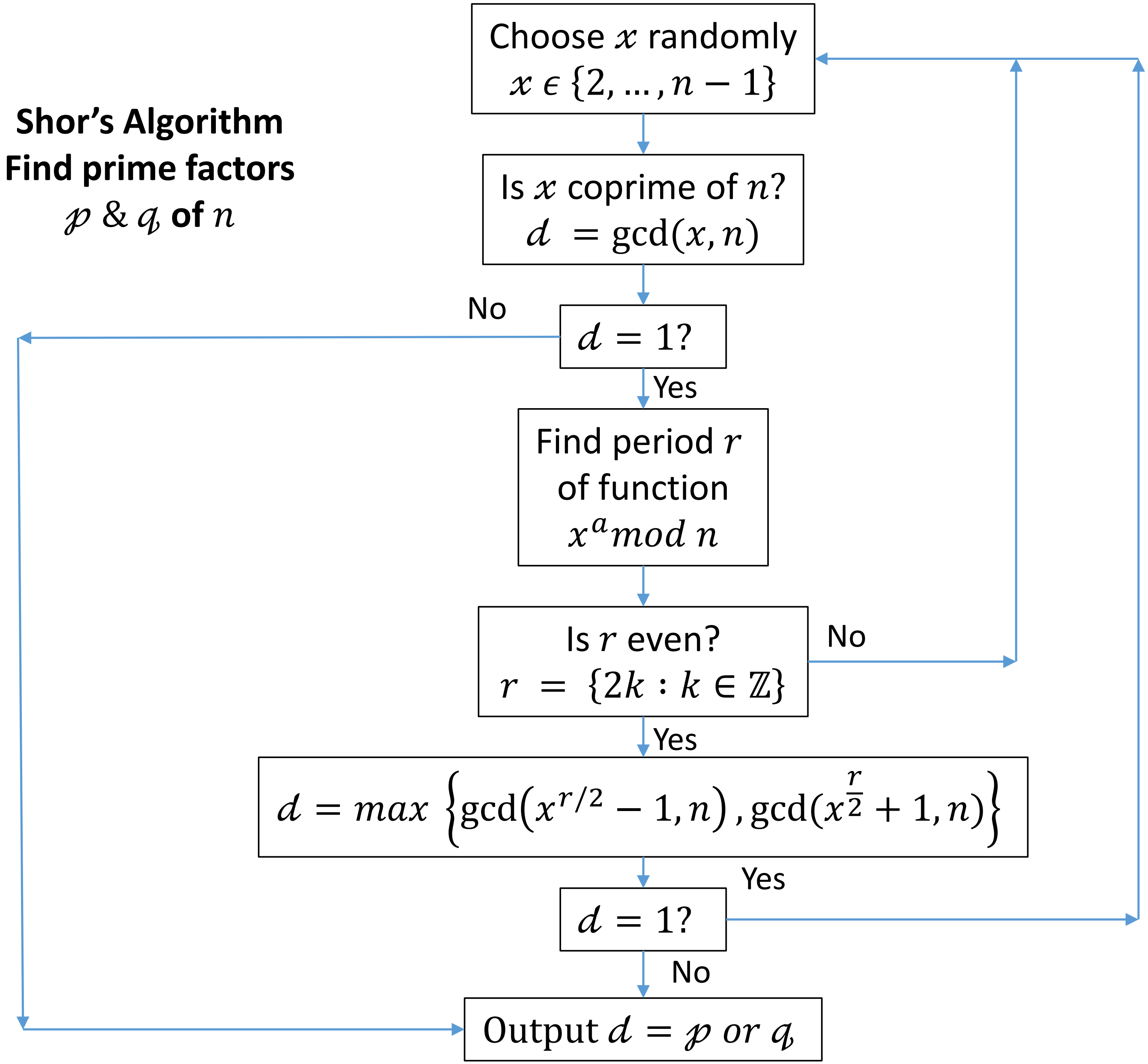
@profwoodward

Structure For Talk

- Quantum computers threaten current public key encryption
- Quantum principle behind Quantum Key Distribution
- Quantum Key Distribution in a nutshell
- Is QKD really the answer to the threat posed by quantum computers

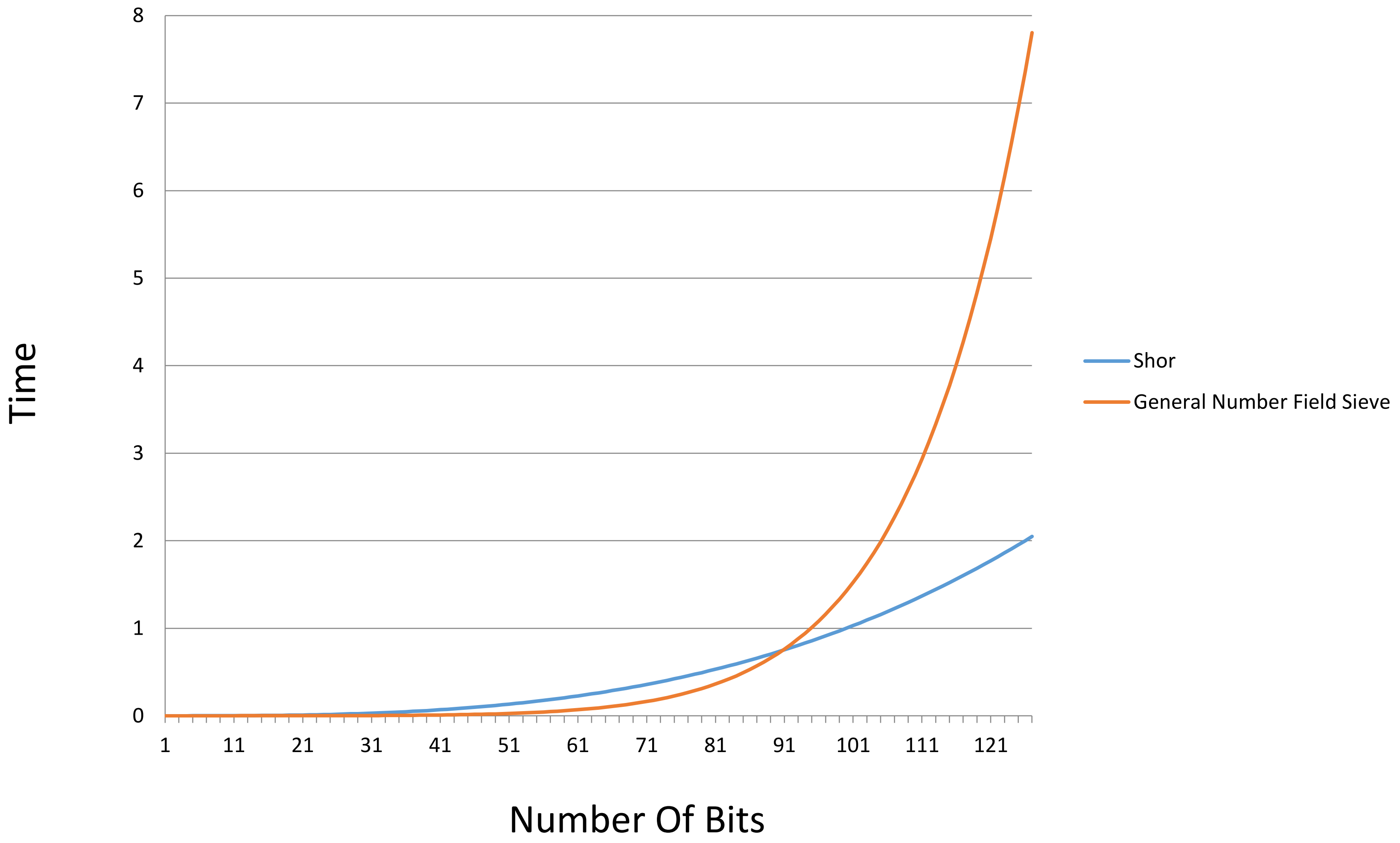
Public Key Encryption

- Arose because of key management problems
- Principle role is to exchange a key securely so that strong symmetric encryption can be conducted
- Public Key Encryption is not intended to encrypt whole messages, only the key – use key in symmetric encryption
- Provides secure key exchange on an insecure channel
- Relies upon mathematical problems that are easy to compute one way but hard in reverse: “computationally secure” not “perfectly secure” eg:
  - RSA
  - Elliptic curve
- Offers more than just Confidentiality – Integrity & Authentication as well

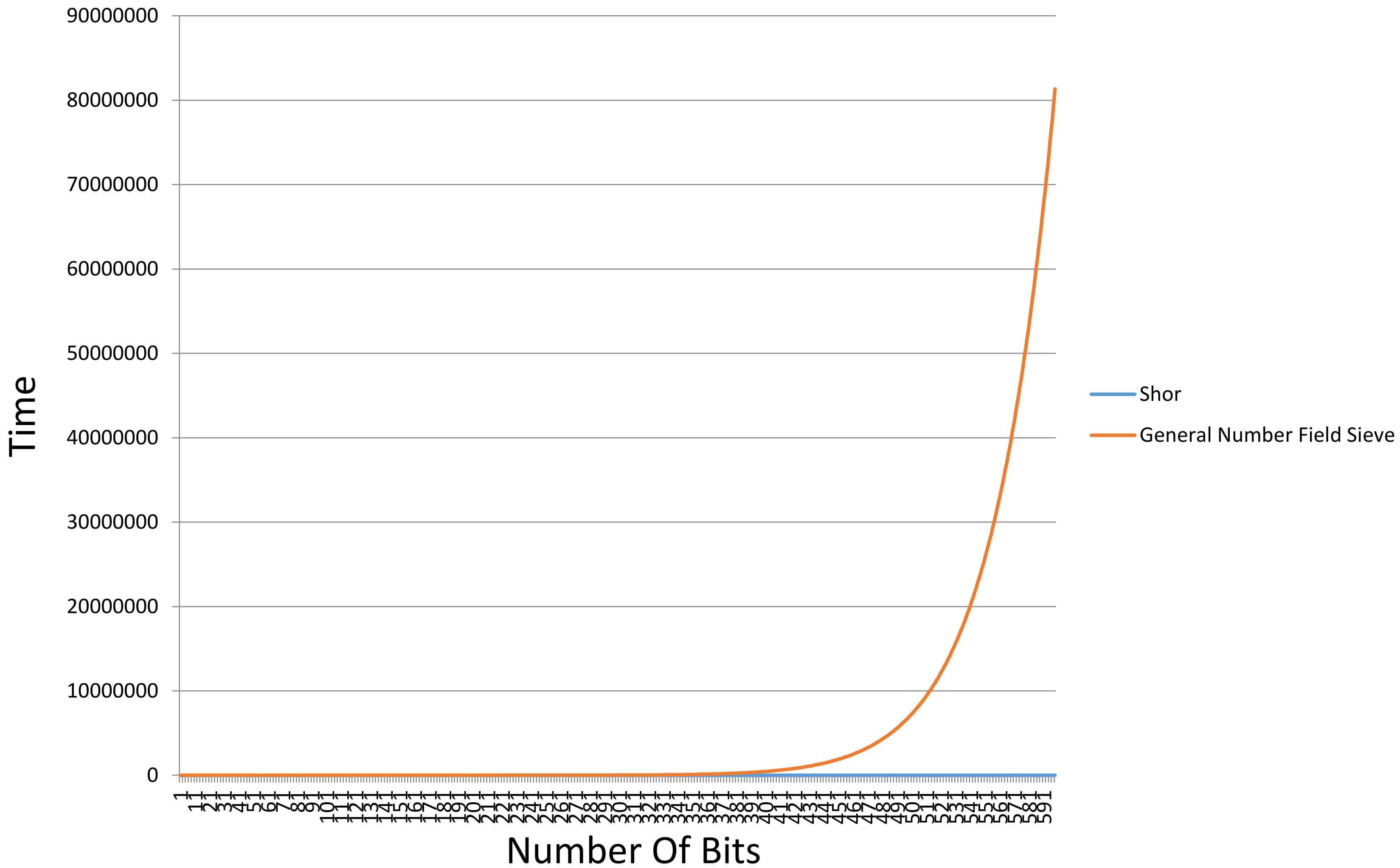

Shor's Algorithm
Find prime factors
p & q of n
Choose x randomly
$x \in \{2, \ldots, n-1\}$
Is x coprime of n?
$d = \gcd(x, n)$
No
$d = 1?$
Yes
Find period r
of function
$x^a \bmod n$
Is r even?
$r = \{2k : k \in \mathbb{Z}\}$
No
Yes
$d = max\left\{\gcd\left(x^{r/2} - 1, n\right), \gcd(x^{\frac{r}{2}} + 1, n)\right\}$
Yes
$d = 1?$
No
Output $d = p$ or q

Quantifying The Speedup

- A k-bit number can be factored in time $O k^3$ using a machine capable of storing 5k +1 qubits
- $O(e^{7.1k^{1/3} (\log k)^{2/3}})$ to factor k-bit number using fastest classical method (General Number Field Sieve)



Time
8
7
6
5
4
3
2
1
0
1
11
21
31
41
51
61
71
81
91
101
111
121
Number Of Bits
Shor
General Number Field Sieve



90000000
80000000
70000000
60000000
50000000
40000000
30000000
20000000
10000000
0
Time
Number Of Bits
Shor
General Number Field Sieve

Recent Insights Into Speeding Up The Classical elements of Shor's Algorithm

Shor's Algorithm and Factoring: Don't Throw Away the Odd Orders

Anna M. Johnston
Juniper Networks
amj at juniper dot net

February 6, 2017

Abstract

Shor's algorithm factors an integer N in two steps. The quantum step computes the order of $a \bmod N$ where a is relatively prime to N. The classical step uses this order to factor N. Descriptions of the classical step require the order, s, to be even and that $a^{s/2} \not\equiv -1 \bmod N$. If s is odd or $a^{s/2} \equiv -1 \bmod N$, then the quantum step is repeated. This paper describes how each prime divisor of the order s, not just 2, can be used to factor N.

1 Sketch of Shor's Algorithm

Shor's[4] algorithm factors a composite integer N, which is not a non-trivial power, in two steps. The first step uses quantum computing to find the order of some integer a modulo N, where $\gcd(a, N) = 1$. In other words, this step finds the smallest positive integer s such that $a^s \equiv 1 \bmod N$.

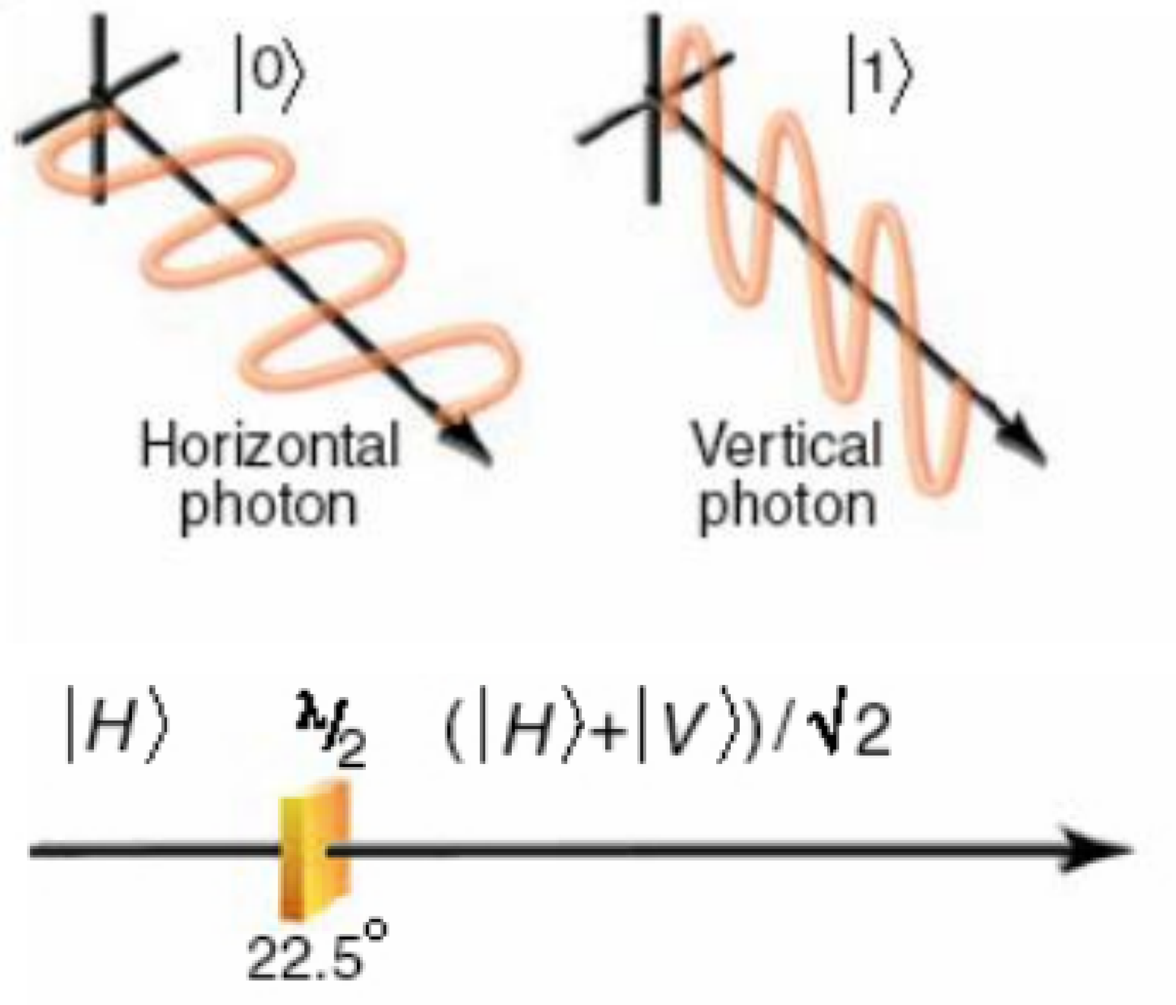
The second step uses the order, s, and classical techniques to factor N. If s is odd or $a^{s/2} \equiv -1 \bmod N$, then the quantum step is repeated. Otherwise, let $b_2 \equiv a^{s/2} \bmod N$, and notice that b_2 has order 2 modulo N. In other words, $b_2^2 \equiv 1 \bmod N$ and

$$\left(b_2^2 - 1\right) \equiv \left(b_2 - 1\right)\left(b_2 + 1\right) \equiv 0 \bmod N.$$

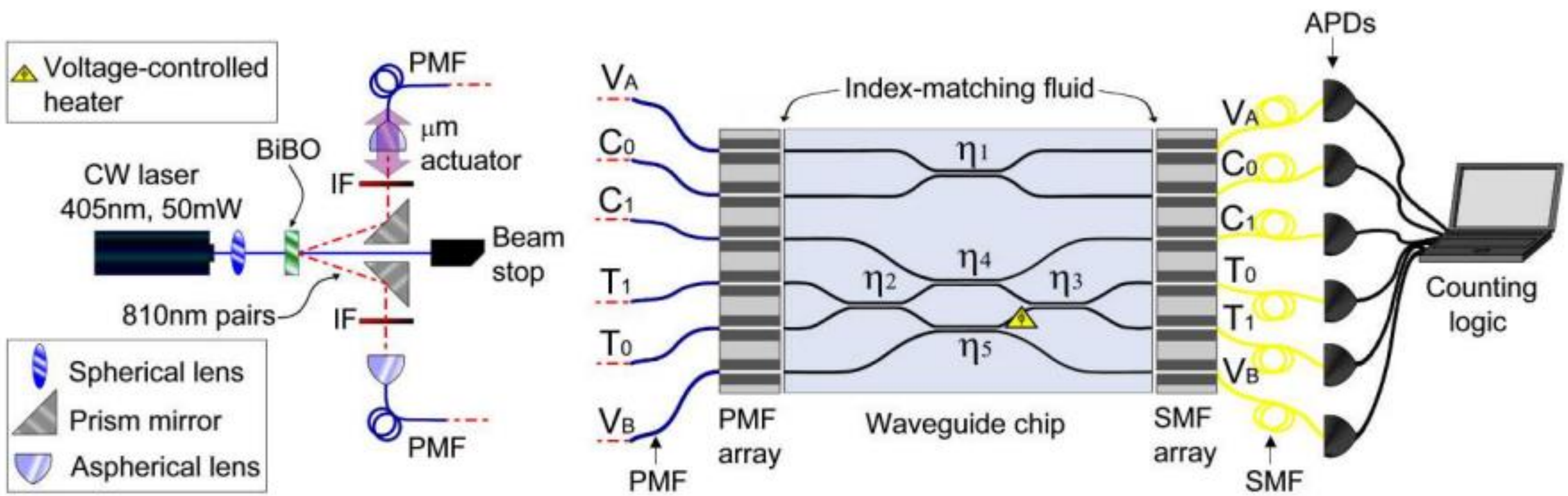
A non-trivial factorization of N is

$$N = \gcd(\left(b_2 - 1\right), N)\gcd(\left(b_2 + 1\right), N).$$

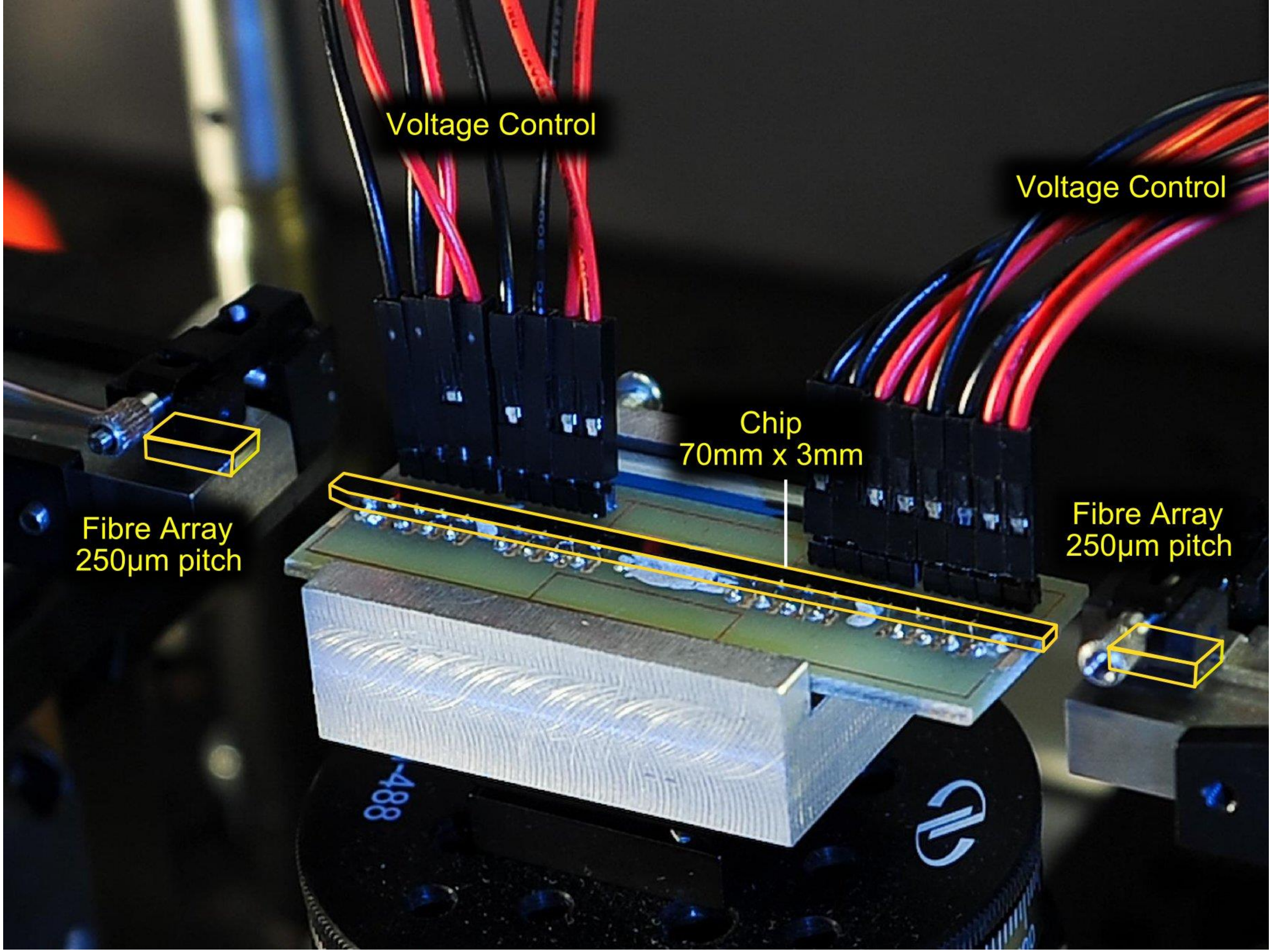
1



Optical Qubits



Reconfigurable Photonic Circuits



Reconfigurable Photonic Circuits

For More….

- https://www.youtube.com/watch?v=aIyxqaJUR7Y

Structure For Talk

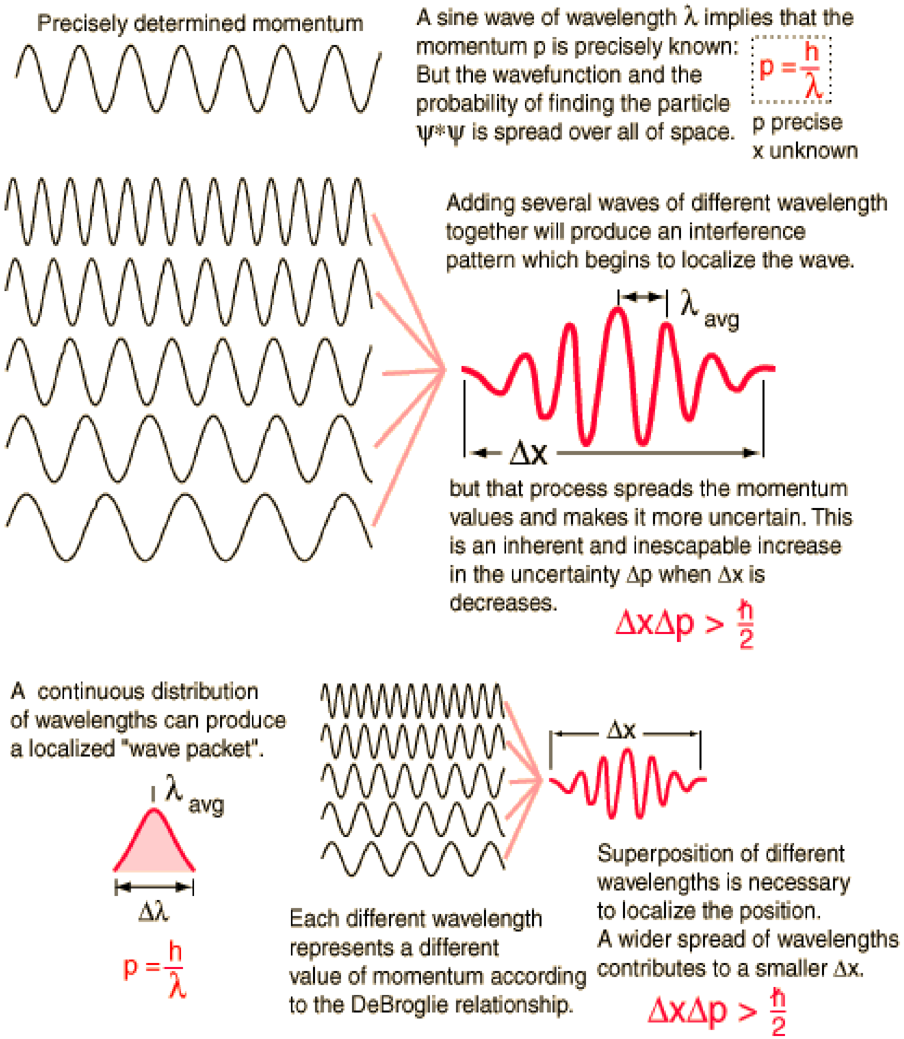
- Quantum computers threaten current public key encryption
- Quantum principle behind Quantum Key Distribution:
  - Particle-wave duality
  - Heisenberg’s principle
  - No-cloning theorem
  - Photon polarisation
  - Bell’s Theorem & Inequalities
- Quantum Key Distribution in a nutshell
- Is QKD really the answer to the threat posed by quantum computers?

WAVE-PARTICLE DUALITY OF LIGHT

In 1924 Einstein wrote:- " There are therefore now two theories of light, both indispensable, and … without any logical connection."

- Light exhibits diffraction and interference phenomena that are *only* explicable in terms of wave properties
  - Diffraction and interference
- Light is always detected as packets (photons); if we look, we never observe half a photon
  - Photoelectric effect
  - Compton effect
- Number of photons proportional to energy density (i.e. to square of electromagnetic field strength)

Uncertainty

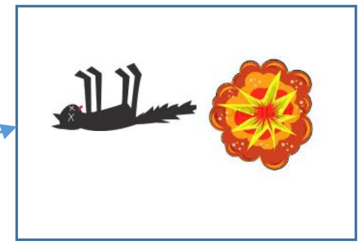


Source: Georgia State University

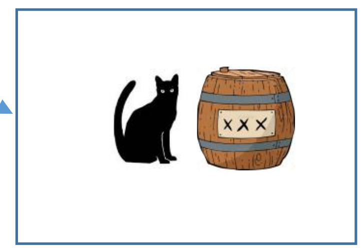

CAUTION: MAY OR MAY NOT CONTAIN LIVE ANIMAL
RADIOACTIVE II
7
POISON
6

Remember Schrodinger's Cat (Simplified)

Cat sits in box with unstable gunpowder that has a probability of exploding

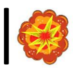


Probability gunpowder explodes



Probability gunpowder <u>doesn't</u> explodes

Principles Behind No Cloning

1. Superposition is linear combination of two possible states simultaneously (ignoring complex probability amplitude complex variables):
   - Gunpowder in superposition = |> + |>
   - $|A\rangle = |A_1\rangle + |A_2\rangle$
2. Composite systems (cat plus gunpowder):
   - $\boxed{?}$ = |> x |> +|> x |>
   - $|AB\rangle = |A_1\rangle \times |B_1\rangle + |A_2\rangle \times |B_2\rangle$
3. Transformation of systems in superposition:
   - $T(|A_1\rangle + |A_2\rangle) = T(|A_1\rangle) + \mathrm{T}(|A_2\rangle)$

Why No Cloning: Proof By Contradiction

- Assuming you could clone you end up with a system with two copies of same superposition which by principle 2:
  - $\text{Clone}(|A_1\rangle + |A_2\rangle) = (|A_1\rangle + |A_2\rangle) \times (|A_1\rangle + |A_2\rangle)$
- But by principle 3 this should be equivalent to:
  - $\text{Clone}|A_1\rangle + \text{Clone}|A_2\rangle = |A_1\rangle \times |A_1\rangle + |A_2\rangle \times |A_2\rangle$
- Yet:
  - $(|A_1\rangle + |A_2\rangle) \times (|A_1\rangle + |A_2\rangle) \neq |A_1\rangle \times |A_1\rangle + |A_2\rangle \times |A_2\rangle$
- Hence, you cannot clone an unknown quantum state

Entanglement

Einstein called this *“spukhafte Fernwirkung”* or *“spooky action at a distance”*

Bell’s Theorem

No physical theory of local hidden variables can ever reproduce all of the predictions of quantum mechanics

III.5 ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

JOHN S. BELL†

I. Introduction

THE paradox of Einstein, Podolsky and Rosen [1] was advanced as an argument that quantum mechanics could not be a complete theory but should be supplemented by additional variables. These additional variables were to restore to the theory causality and locality [2]. In this note that idea will be formulated mathematically and shown to be incompatible with the statistical predictions of quantum mechanics. It is the requirement of locality, or more precisely that the result of a measurement on one system be unaffected by operations on a distant system with which it has interacted in the past, that creates the essential difficulty. There have been attempts [3] to show that even without such a separability or locality requirement no "hidden variable" interpretation of quantum mechanics is possible. These attempts have been examined elsewhere [4] and found wanting. Moreover, a hidden variable interpretation of elementary quantum theory [5] has been explicitly constructed. That particular interpretation has indeed a grossly non-local structure. This is characteristic, according to the result to be proved here, of any such theory which reproduces exactly the quantum mechanical predictions.

II. Formulation

With the example advocated by Bohm and Aharonov [6], the EPR argument is the following. Consider a pair of spin one-half particles formed somehow in the singlet spin state and moving freely in opposite directions. Measurements can be made, say by Stern-Gerlach magnets, on selected components of the spins $\vec{\sigma}_1$ and $\vec{\sigma}_2$. If measurement of the component $\vec{\sigma}_1 \cdot \vec{a}$, where $\vec{a}$ is some unit vector, yields the value $+1$ then, according to quantum mechanics, measurement of $\vec{\sigma}_2 \cdot \vec{a}$ must yield the value -1 and vice versa. Now we make the hypothesis [2], and it seems one at least worth considering, that if the two measurements are made at places remote from one another the orientation of one magnet does not influence the result obtained with the other. Since we can predict in advance the result of measuring any chosen component of $\vec{\sigma}_2$, by previously measuring the same component of $\vec{\sigma}_1$, it follows that the result of any such measurement must actually be predetermined. Since the initial quantum mechanical wave function does *not* determine the result of an individual measurement, this predetermination implies the possibility of a more complete specification of the state.

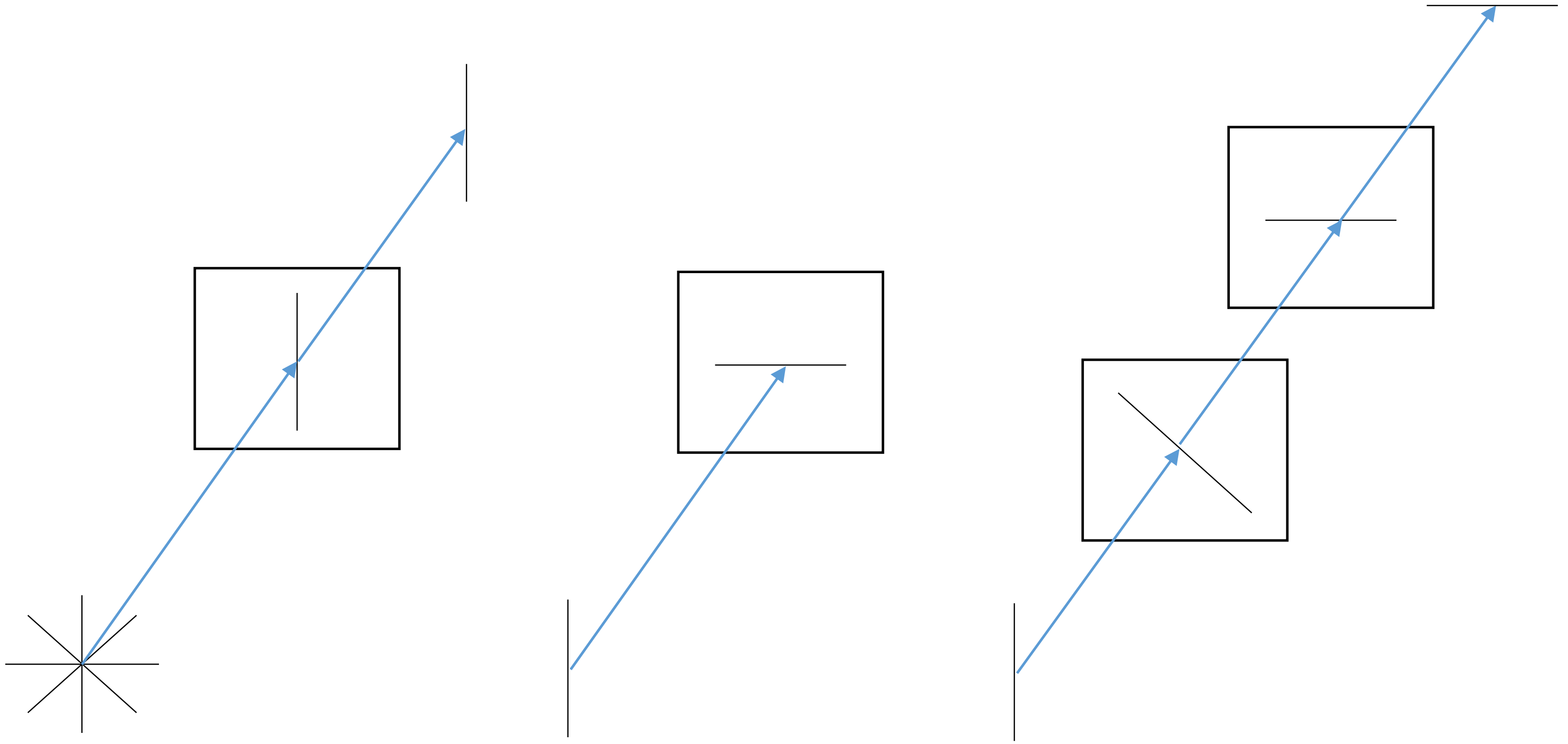
Let this more complete specification be effected by means of parameters λ. It is a matter of indifference in the following whether λ denotes a single variable or a set, or even a set of functions, and whether the variables are discrete or continuous. However, we write as if λ were a single continuous parameter. The result A of measuring $\vec{\sigma}_1 \cdot \vec{a}$ is then determined by $\vec{a}$ and λ, and the result B of measuring $\vec{\sigma}_2 \cdot \vec{b}$ in the same instance is determined by $\vec{b}$ and λ, and

*Work supported in part by the U.S. Atomic Energy Commission

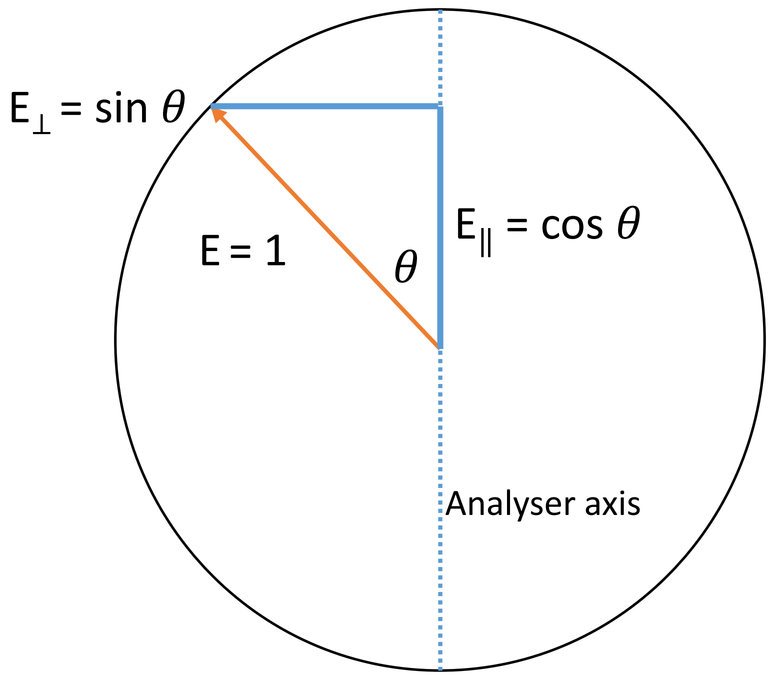
†On leave of absence from SLAC and CERN

Originally published in *Physics*, *1*, 195-200 (1964).

Photon Polarisation

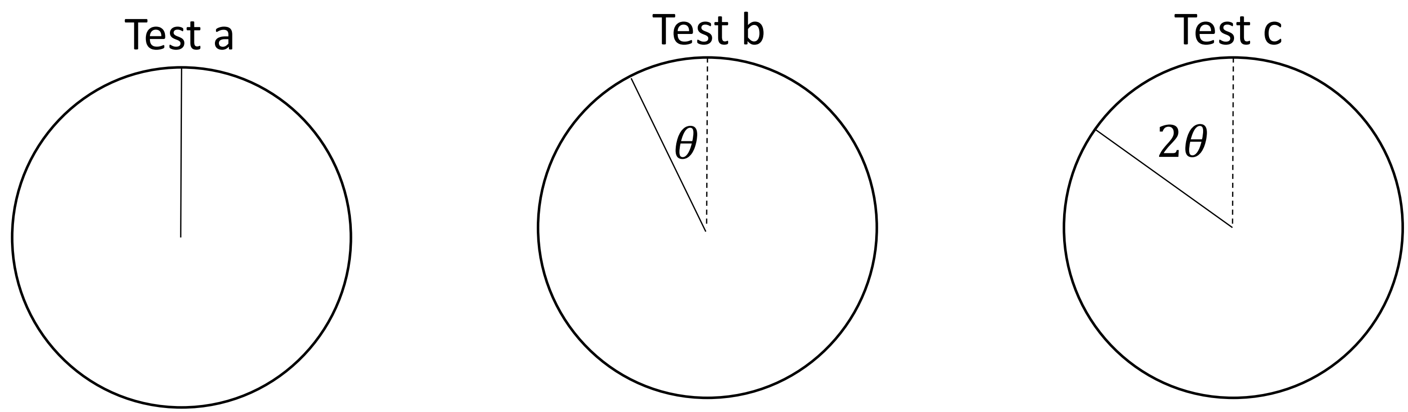


Photon Polarisation



- Transmitted field intensity $\sim \cos^2\theta$
- Blocked field intensity $\sim \sin^2\theta$
- But photons are discrete so either pass or fail $\therefore$ probability of photon passing is:
  - Pass $\sim \cos^2\theta$
  - Fail $\sim \sin^2\theta$
- And we know (simple trig formula):
  - $\cos^2\theta + \sin^2\theta = 1$
  - $P(\text{fail}) + P(\text{pass}) = 1$

Bell's Inequality On Polarised Photons



Pass: a=1, a
Fail: a=0, $\bar{a}$

Pass: b=1, b
Fail: b=0, $\bar{b}$

Pass: c=1, c
Fail: c=0, $\bar{c}$

If there is a hidden local variable, there are only 8 possible outcomes of 3 tests

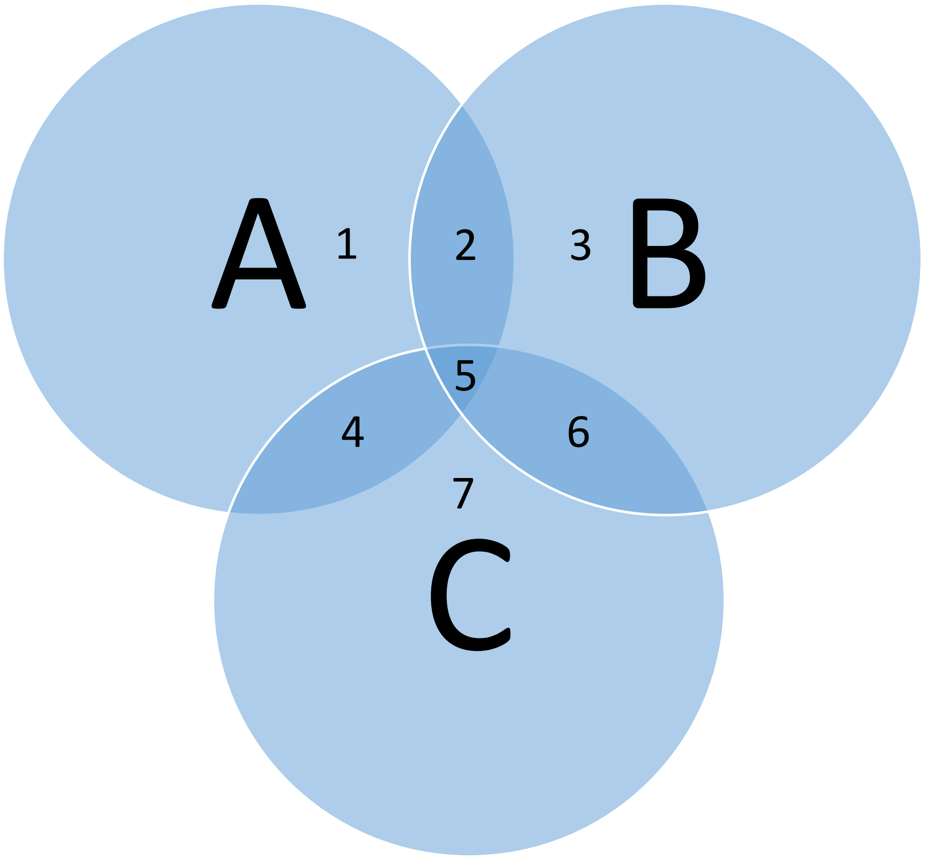
a	b	c	$a\bar{b}$	$b\bar{c}$	$a\bar{c}$
0	0	0			
0	0	1			
0	1	0		+	
0	1	1			
1	0	0	+		+
1	0	1	+		
1	1	0		+	+
1	1	1			

$$N(a\bar{c}) + N(b\bar{c}) \geq N(a\bar{c})$$

For large numbers

$$P(a\bar{c}) + P(b\bar{c}) \geq P(a\bar{c})$$

Bell’s Inequality

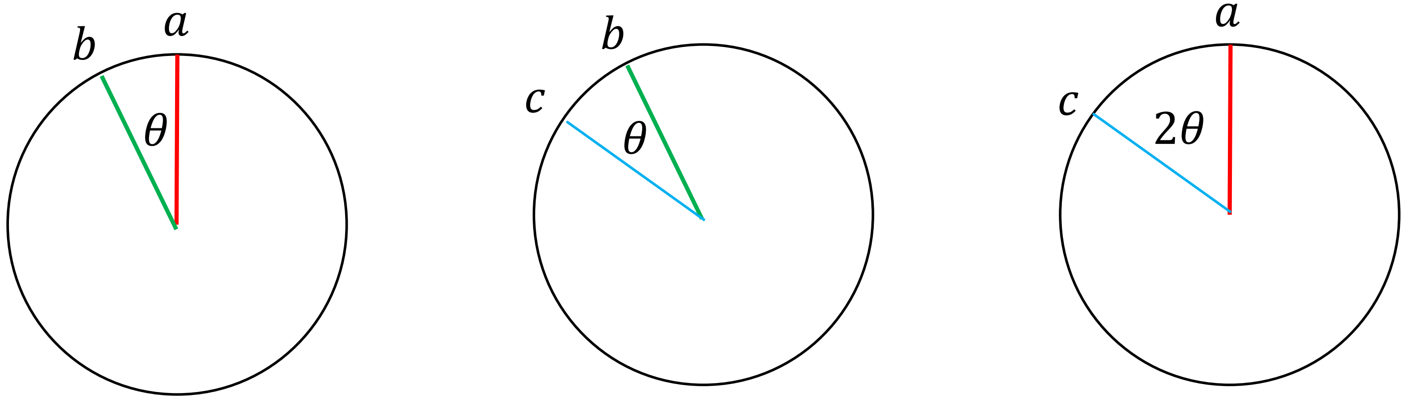


(A not B) + (B not C) $\geq$ A not C

$$(1+4) \ + \ (3+2) \ \geq 1+2$$

$$(1+2) \ + \ 3+4 \ \geq 1+2$$

Bell's Inequality

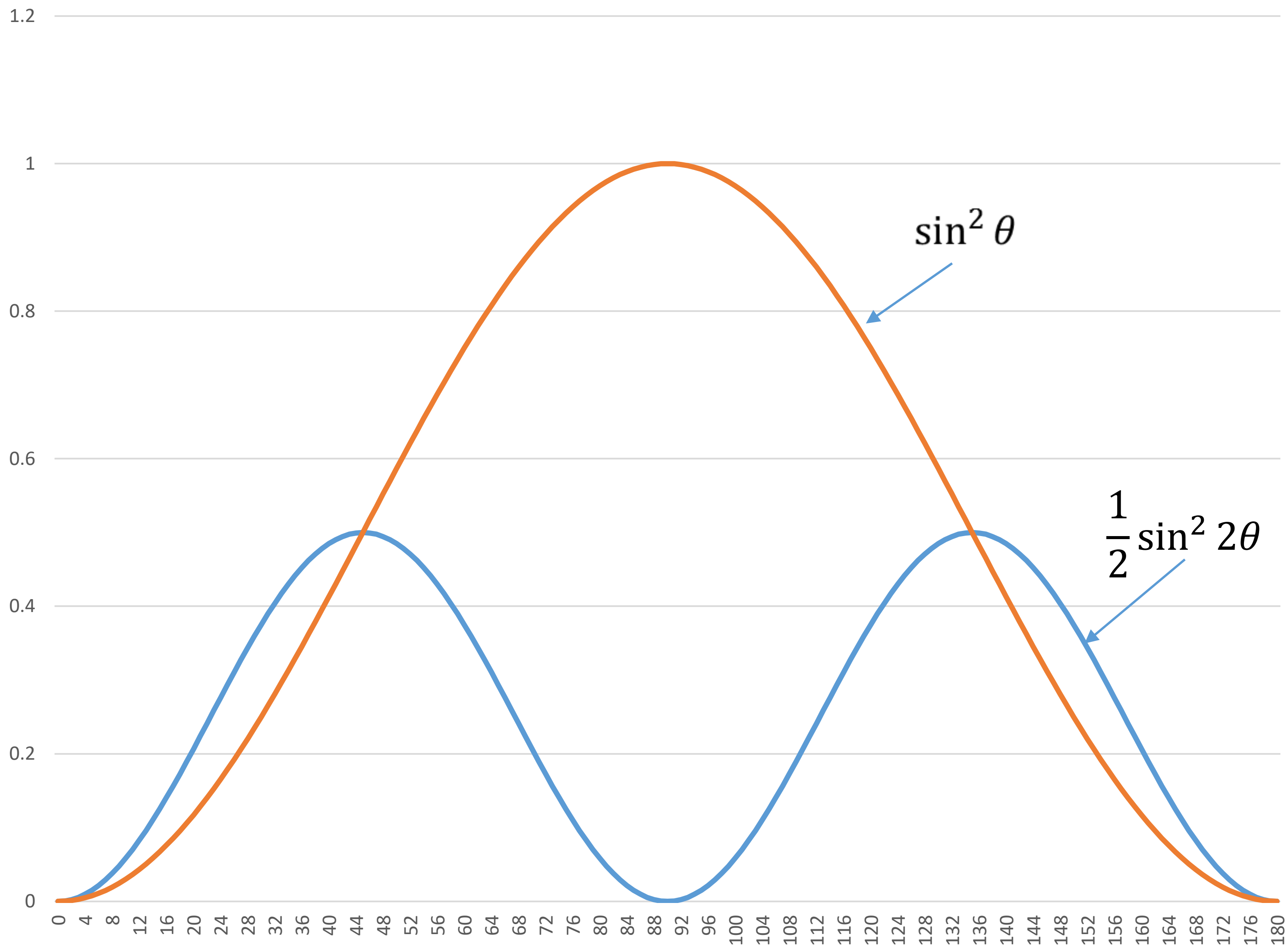


$$P(a\bar{b}) = \frac{1}{2}\sin^2\theta \qquad P(b\bar{c}) = \frac{1}{2}\sin^2\theta \qquad P(a\bar{c}) = \frac{1}{2}\sin^2 2\theta$$

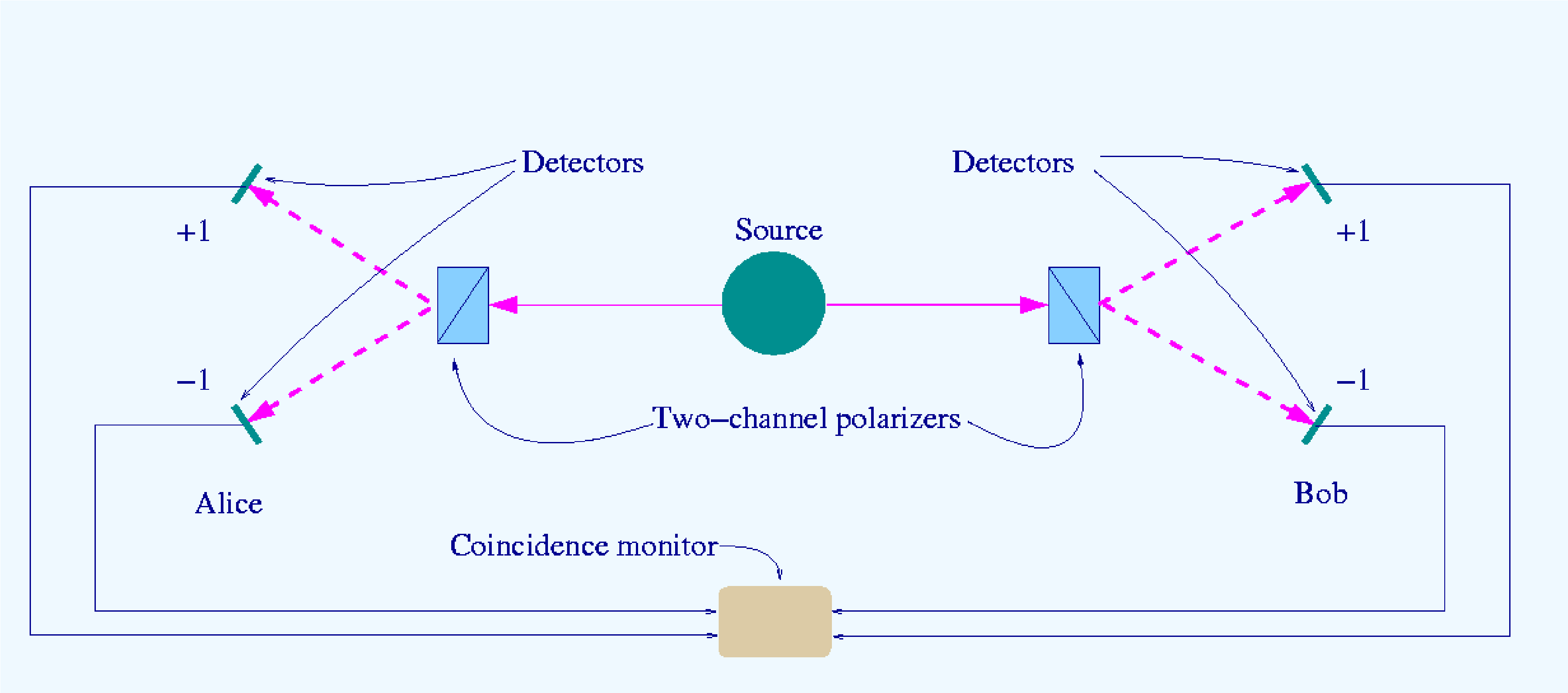
$$P(a\bar{b}) \quad + \quad P(b\bar{c}) \quad \geq \quad P(a\bar{c})$$

$$\sin^2\theta \geq \frac{1}{2}\sin^2 2\theta$$

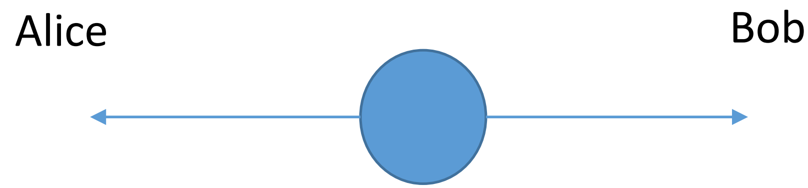
Bell's Inequality Is Violated

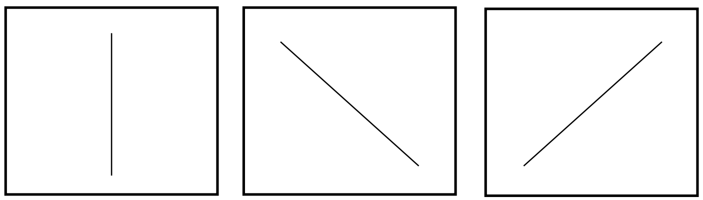


Experiment For Proving Bell’s Theorem



Bell's Inequality Experimentally





Same inequality $\geq 1/3$

But experiment measures ≥ 0.25

1	2	3
Y	Y	Y
Y	Y	N
Y	N	Y
Y	N	N
N	Y	Y
N	Y	N
N	N	Y
N	N	N

1&2	2&3	1&3
S	S	S
S	D	D
D	D	S
D	S	D
D	S	D
D	D	S
S	D	D
S	S	S

1/3

Other Quantum Phenomenon Also Relevant

Quantum Cloning Machines and the Applications

Heng Fan,[1,2,*] Yi-Nan Wang,[3] Li Jing,[3] Jie-Dong Yue,[1] Han-Duo Shi,[3] Yong-Liang Zhang,[3] and Liang-Zhu Mu[3]
[1]*Beijing National Laboratory for Condensed Matter Physics, Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China*
[2]*Collaborative Innovation Center of Quantum Matter, Beijing 100190, China*
[3]*School of Physics, Peking University, Beijing 100871, China*

(Dated: August 5, 2014)

No-cloning theorem is fundamental for quantum mechanics and for quantum information science that states an unknown quantum state cannot be cloned perfectly. However, we can try to clone a quantum state approximately with the optimal fidelity, or instead, we can try to clone it perfectly with the largest probability. Thus various quantum cloning machines have been designed for different quantum information protocols. Specifically, quantum cloning machines can be designed to analyze the security of quantum key distribution protocols such as BB84 protocol, six-state protocol, B92 protocol and their generalizations. Some well-known quantum cloning machines include universal quantum cloning machine, phase-covariant cloning machine, the asymmetric quantum cloning machine and the probabilistic quantum cloning machine etc. In the past years, much progress has been made in studying quantum cloning machines and their applications and implementations, both theoretically and experimentally. In this review, we will give a complete description of those important developments about quantum cloning and some related topics. On the other hand, this review is self-consistent, and in particular, we try to present some detailed formulations so that further study can be taken based on those results.

PACS numbers: 03.67.Ac, 03.65.Aa, 03.67.Dd, 03.65.Ta

Contents

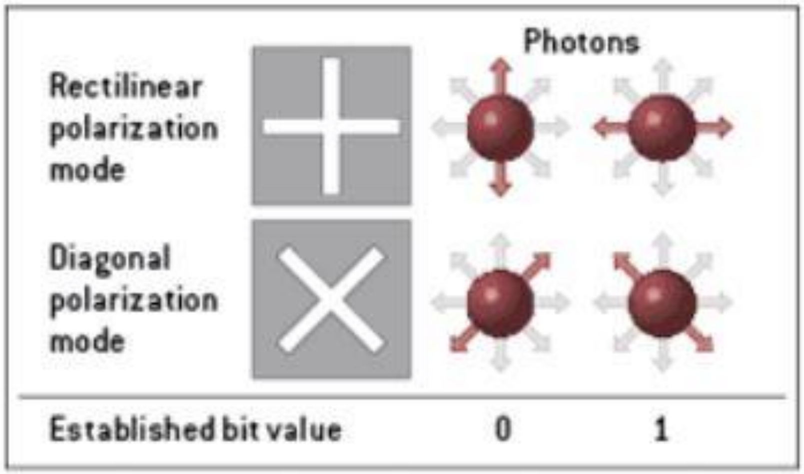
*Electronic address: hfan@iphy.ac.cn

- No-broadcasting theorem
- No-broadcasting for correlations
- Unified information theoretic no-cloning theorem
- No-cloning and no-signalling
- No-cloning for unitary operators
- Teleportation

Structure For Talk

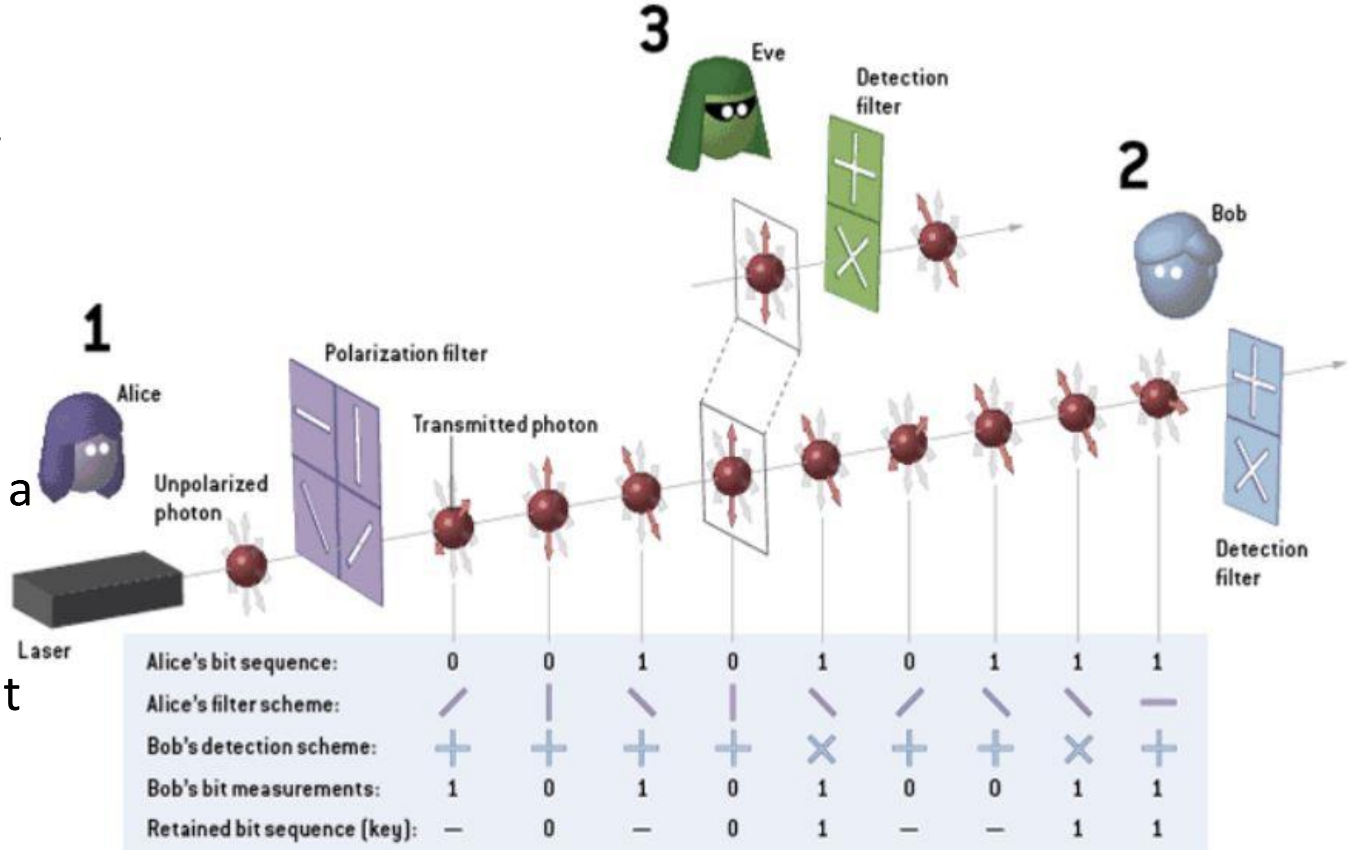
- Quantum computers threaten current public key encryption
- Quantum principle behind Quantum Key Distribution
- Quantum Key Distribution in a nutshell
- Is QKD really the answer to the threat posed by quantum computers

Quantum Key Distribution

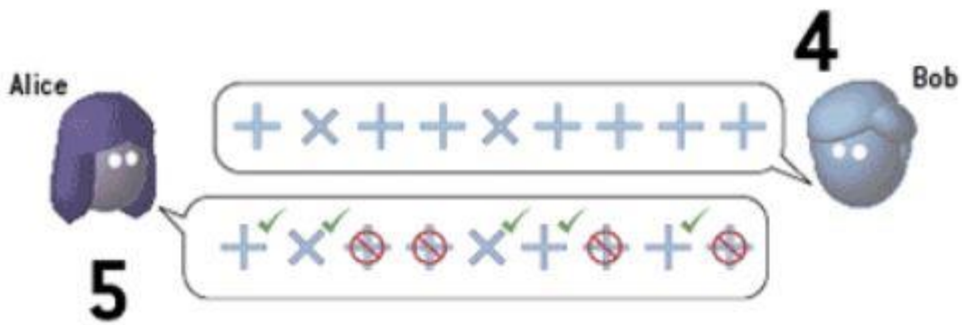


- Invented by Charles Bennett & Gilles Brassard in 1980s: the BB84 protocol
- Transmit your secret key as polarized photons
- Polarization can be either rectilinear or diagonal
- 0 or 1 can be transmitted using either polarization

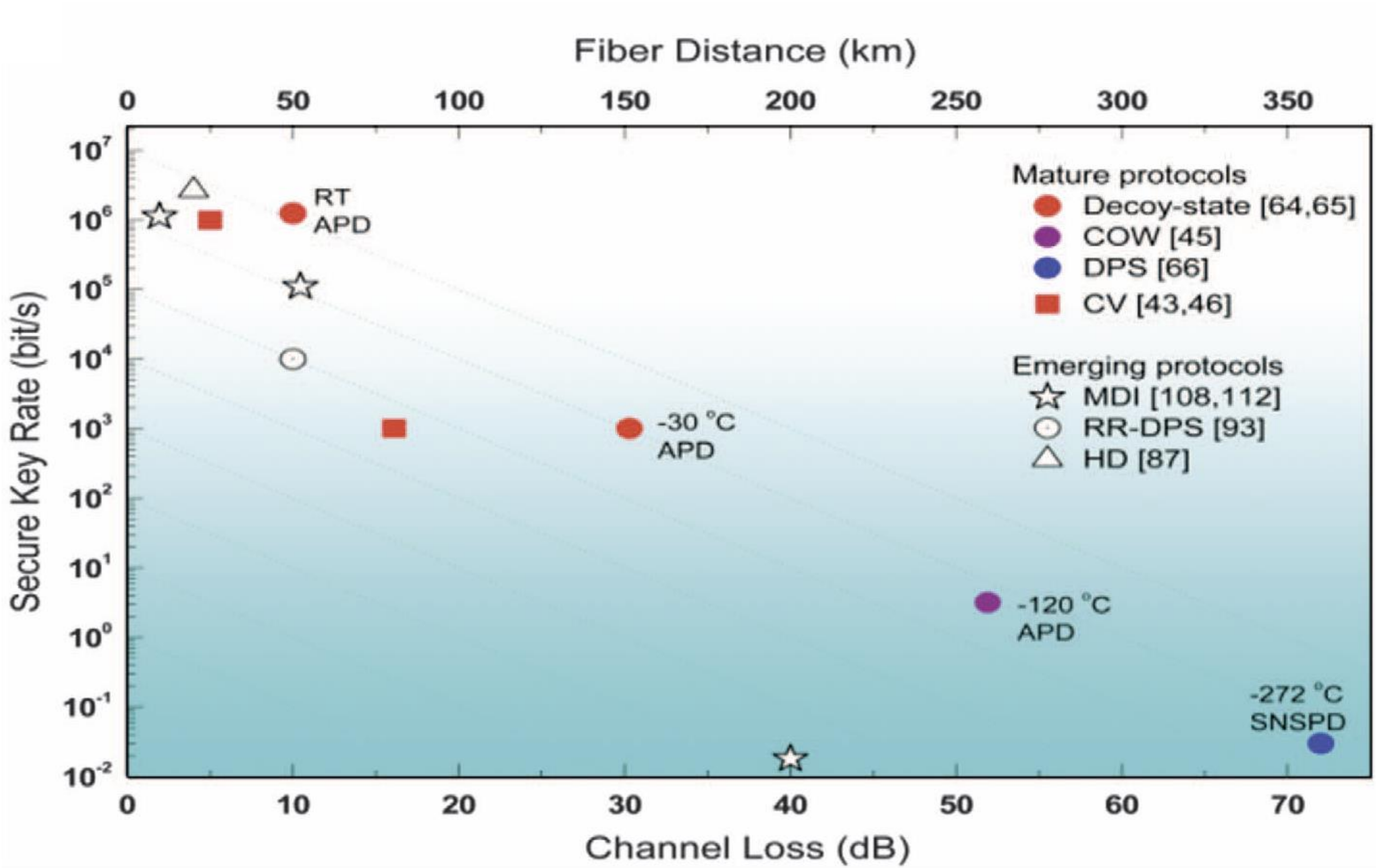
1. Alice sends 0 or 1 through either orientation making record of which was used
2. Bob randomly decides whether to detect his photons through a rectilinear or a diagonal slot
3. If Eve intercepts it can introduce errors by forcing what should be a rectilinear orientation to be diagonal and vice versa



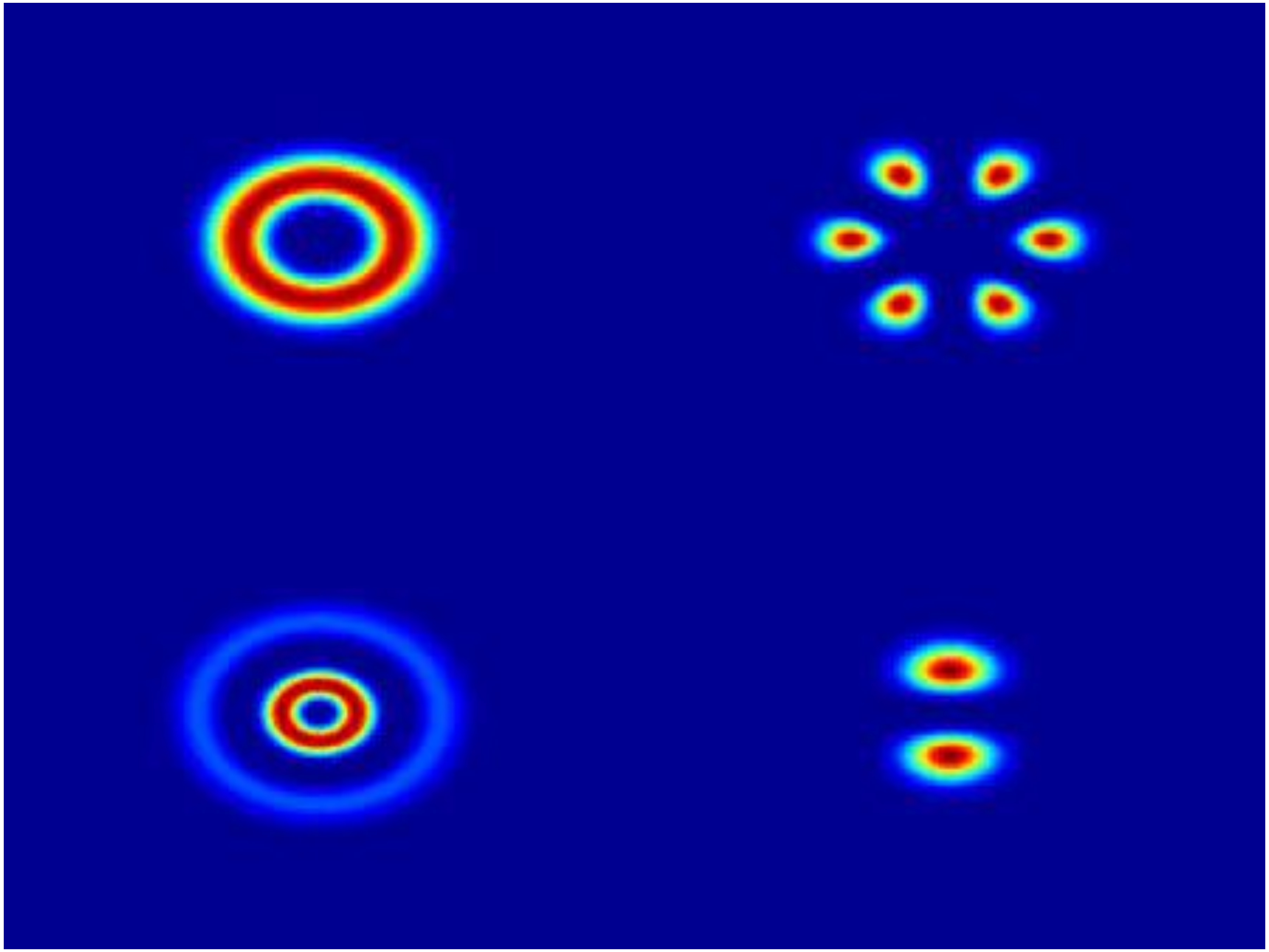
4. Once all photons received Bob tells Alice which polarizations he used (but not the values he derived)
5. Alice tells Bob which were correct and it is these "bits" that they use for their secret key



Limitation Of Using Light



Atmospheric Effects



Active Research Into Entanglement Decays Due To Perturbations

nature physics

ARTICLES

PUBLISHED ONLINE: 23 JANUARY 2017 | DOI: 10.1038/NPHYS4003

Characterizing quantum channels with non-separable states of classical light

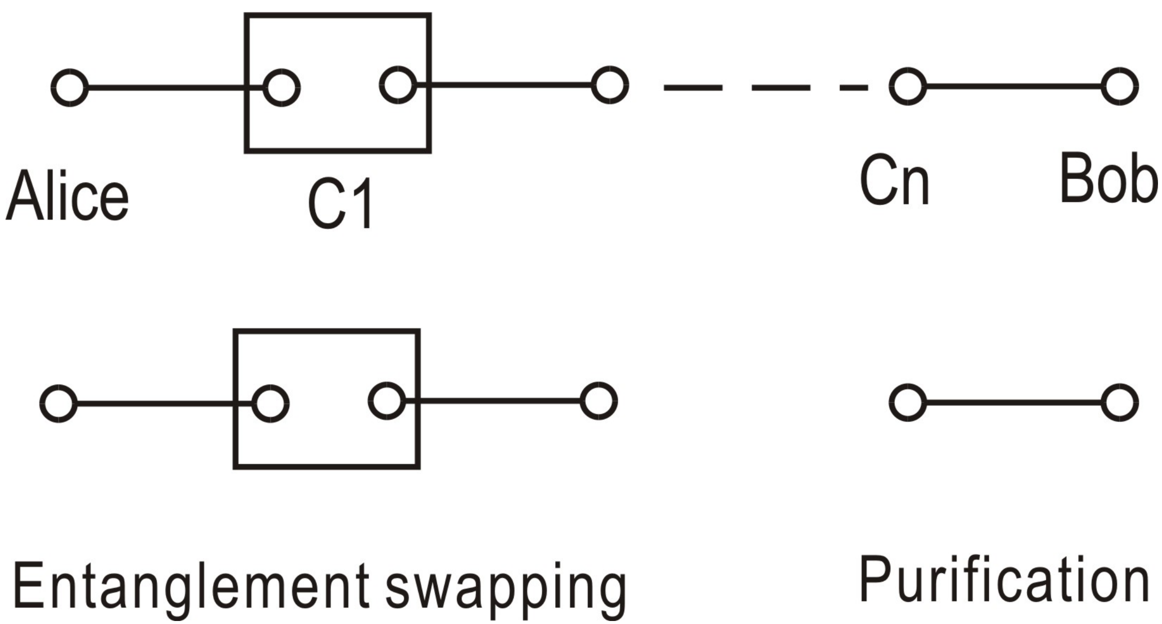
Bienvenu Ndagano[1], Benjamin Perez-Garcia[1,2], Filippus S. Roux[1,3], Melanie McLaren[1], Carmelo Rosales-Guzman[1], Yingwen Zhang[4†], Othmane Mouane[1], Raul I. Hernandez-Aranda[2], Thomas Konrad[5] and Andrew Forbes[1*]

High-dimensional entanglement with spatial modes of light promises increased security and information capacity over quantum channels. Unfortunately, entanglement decays due to perturbations, corrupting quantum links that cannot be repaired without performing quantum tomography on the channel. Paradoxically, the channel tomography itself is not possible without a working link. Here we overcome this problem with a robust approach to characterize quantum channels by means of classical light. Using free-space communication in a turbulent atmosphere as an example, we show that the state evolution of classically entangled degrees of freedom is equivalent to that of quantum entangled photons, thus providing new physical insights into the notion of classical entanglement. The analysis of quantum channels by means of classical light in real time unravels stochastic dynamics in terms of pure state trajectories, and thus enables precise quantum error correction in short- and long-haul optical communication, in both free space and fibre.

Drawbacks and Quantum Repeater

Decoherence →**Quantum Entanglement Purification**
Background Noise →**Quantum Entanglement Swapping**

} **Quantum Repeater**



H.-J. Briegel, et al., Phys. Rev. Lett. 81, 5932, 1998.

Entanglement & Bell's Theorem?

PHYSICAL REVIEW LETTERS

VOLUME 67 | 5 AUGUST 1991 | NUMBER 6

Quantum Cryptography Based on Bell's Theorem

Artur K. Ekert

Merton College and Physics Department, Oxford University, Oxford OX1 3PU, United Kingdom

(Received 18 April 1991)

Practical application of the generalized Bell's theorem in the so-called key distribution process in cryptography is reported. The proposed scheme is based on the Bohm's version of the Einstein-Podolsky-Rosen *gedanken experiment* and Bell's theorem is used to test for eavesdropping.

PACS numbers: 03.65.Bz, 42.80.Sa, 89.70.+c

Cryptography, despite a colorful history that goes back to 400 B.C., only became part of mathematics and information theory this century, in the late 1940s, mainly due to the seminal papers of Shannon [1]. Today, one can briefly define cryptography as a mathematical system of transforming information so that it is unintelligible and therefore useless to those who are not meant to have access to it. However, as the computational process associated with transforming the information is always performed by physical means, one cannot separate the mathematical structure from the underlying laws of physics that govern the process of computation [2]. Deutsch has shown that quantum physics enriches our computational possibilities far beyond classical Turing machines [2], and current work in quantum cryptography originated by Bennett and Brassard provides a good example of this fact [3].

In this paper I will present a method in which the security of the so-called key distribution process in cryptography depends on the completeness of quantum mechanics. Here completeness means that quantum description provides maximum possible information about any system under consideration. The proposed scheme is based on the Bohm's well-known version of the Einstein-Podolsky-Rosen *gedanken experiment* [4]; the generalized Bell's theorem (Clauser-Horne-Shimony-Holt inequalities) [5] is used to test for eavesdropping. From a theoretical point of view the scheme provides an interesting and new extension of Bennett and Brassard's original idea, and from an experimental perspective offers a practical realization by a small modification of experiments that were set up to test Bell's theorem. Before I proceed any further let me first introduce some basic notions of cryptography.

Originally the security of a cryptotext depended on the secrecy of the entire encrypting and decrypting procedures; however, today we use ciphers for which the algorithm for encrypting and decrypting could be revealed to anybody without compromising the security of a particular cryptogram. In such ciphers a set of specific parameters, called a *key*, is supplied together with the plaintext as an input to the encrypting algorithm, and together with the cryptogram as an input to the decrypting algorithm. The encrypting and decrypting algorithms are publicly announced; the security of the cryptogram depends entirely on the secrecy of the key, and this key, which is very important, may consist of any *randomly chosen*, sufficiently long string of bits. Once the key is established, subsequent communication involves sending cryptograms over a public channel which is vulnerable to total passive interception (e.g., public announcement in mass media). However, in order to establish the key, two users, who share no secret information initially, must at a certain stage of communication use a reliable and a very secure channel. Since the interception is a set of measurements performed by the eavesdropper on this channel, however difficult this might be from a technological point of view, *in principle* any classical channel can always be passively monitored, without the legitimate users being aware that any eavesdropping has taken place. This is not so for quantum channels [3]. In the following I describe a quantum channel which distributes the key

Ekert 91 Protocol

1. A source emits pairs of qubits in a maximally entangled state like:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle|\leftrightarrow\rangle + |\leftrightarrow\rangle|\updownarrow\rangle\right)$$

2. Alice and Bob choose randomly between three bases, obtained by rotating the horizontal-vertical basis around the z-axis by angles :

$$\begin{array}{l} \phi_1^a = 0 \\ \phi_2^a = \frac{1}{8}\pi \\ \phi_3^a = \frac{1}{4}\pi \end{array} \quad \text{for Alice and} \qquad \begin{array}{l} \phi_1^b = 0 \\ \phi_2^b = \frac{1}{8}\pi \\ \phi_4^b = -\frac{1}{8}\pi \end{array} \quad \text{for Bob.}$$

After the transmission has taken place, Alice and Bob release publicly which basis they have chosen for each measurement. They separate the measurements into three groups:

- First group: Consisting of measurements using different orientation of the analysers.

- Second group: Consisting of measurements using the same orientation of the analysers.

- Third group: Consisting of measurements in which at least one of them failed to register a particle.

The first group is used to test Bell's inequalities and the second group to establish a secure key, while the third group is discarded.

Finally, Alice and Bob announce publicly only their results of the first group. Thus, they can check if eavesdropping has taken place. If no eavesdropper has perturbed the system, Alice and Bob can use the measurements of the second group to obtain a secret string of bits ie a key.

Ekert 91 Protocol Simplified

1. Alice and Bob share an entangled photon pair in the state $\left|\Psi^-\right\rangle$;

2. Alice and Bob perform measurements and register the outcomes of the measurements in one of three bases, obtained by rotating the basis around the z-axis by angles $\left|\Phi_1^a\right\rangle = 0$, $\left|\Phi_2^a\right\rangle = \frac{1}{4}\pi$, $\left|\Phi_3^a\right\rangle = \frac{1}{8}\pi$ for Alice and by angles, $\left|\Phi_1^b\right\rangle = 0$ $\left|\Phi_2^b\right\rangle = -\frac{1}{8}\pi$, $\left|\Phi_3^b\right\rangle = \frac{1}{8}\pi$ for Bob.

3. The users choose their bases randomly and independently for each pair.

4. The measurements with the same angle are used as keys and the others are used to check the Bell inequality.

5. If the inequality is violated, there is no eve and the key can be used. Otherwise, they discard all the keys.

Ekert 91 and BB84 States

$U \otimes I$

$$\left|\Psi_E\right\rangle = \frac{1}{\sqrt{2}}\,|\,0>|\,0> + \frac{1}{\sqrt{2}}\,|\,1>|\,1>$$

$$\left|\Psi_{BB}\right\rangle = \frac{1}{2}\left|0\right\rangle\left|\rightarrow\right\rangle + \frac{1}{2}\left|1\right\rangle\left|\uparrow\right\rangle + \frac{1}{2}\left|2\right\rangle\left|\nwarrow\right\rangle \frac{1}{2}\left|3\right\rangle\left|\nearrow\right\rangle$$

$$\begin{cases} U\,|\,0> = \dfrac{1}{\sqrt{2}}\left|0\right\rangle - \dfrac{1}{2}\left|2\right\rangle + \dfrac{1}{2}\left|3\right\rangle \\ U\,|\,1> = \dfrac{1}{\sqrt{2}}\left|1\right\rangle + \dfrac{1}{2}\left|2\right\rangle + \dfrac{1}{2}\left|3\right\rangle \end{cases}$$

Security Concerns in QKD (1)

- Noisy quantum channels:
  - Alice and Bob measurements not perfectly correlated – is it noisy imperfect equipment or an eavesdropper?
  - Alice and Bob would not want to discard every transmission that wasn't error free since there likely will always be some natural error not caused by Eve
  - Use Privacy Amplification – transform the key to some form unknown to Eve which abstracts key to a form unknowable by Eve unless she has full original key

Privacy Amplification

- A hash function *h* of the following class is randomly and publicly chosen:

$$h : \{0,1\}^n \rightarrow \{0,1\}^{n-l-s}$$

- With *n* bits where Eve's expected deterministic information is *l* bits, and an arbitrary security parameter *s*, Eve's expected information on *h(x)* will be less than

$$\frac{2^{-s}}{\ln 2}$$

- *h(x)* will be the final shared key between Alice and Bob

Security Concerns in QKD (2)

- Photon Number Splitting (PNS):
  - Difficult to produce & detect single photons
  - Often use laser produces small amounts of coherent light – multiple photons
  - Eve splits off a photon & passes remainder on to Bob – Eve can measure her photons without disturbing Bob's
  - Can send decoy pulses - Lo, H., Ma, X., Chen, K., "Decoy state quantum key distribution.", Phys. Rev. Lett. 94, 230504, 2005

Solution to PNS

- SARG04 Protocol:
  - [Scarani, Acin, Ribordy, Gisin, PRL 92, 057901 (2004)]
- Decoy State Method
  - [Hwang, PRL 91, 057901 (2003)]
  - [Wang, PRL 94, 230503 (2005)]
  - [Lo, Ma and Chen PRL 94, 230504 (2005)]
- Strong Reference Pulse Scheme
  - [Huttner, Imoto, Gisin, Mor, PRA 51, 1863 (1995)]

Single Photon Systems Coming

Interesting Developments In Physics

ARTICLES
PUBLISHED ONLINE: 12 OCTOBER 2015 | DOI: 10.1038/NPHOTON.2015.195

nature photonics

Undoing the effect of loss on quantum entanglement

Alexander E. Ulanov[1,2,3†], Ilya A. Fedorov[1,4†], Anastasia A. Pushkina[1,3,4], Yury V. Kurochkin[1], Timothy C. Ralph[5] and A. I. Lvovsky[1,2,4,6,7*]

Entanglement distillation, the purpose of which is to probabilistically increase the strength and purity of quantum entanglement, is a primary element of many quantum communication and computation protocols. It is particularly necessary in quantum repeaters in order to counter the degradation of entanglement that inevitably occurs due to losses in communication lines. Here, we distil the Einstein–Podolsky–Rosen state of light, the workhorse of continuous-variable entanglement, using noiseless amplification. The advantage of our technique is that it permits recovering a macroscopic level of entanglement, however low the initial entanglement or however high the loss may be. Experimentally, we recover the original entanglement level after one of the Einstein–Podolsky–Rosen modes has experienced a loss factor of 20. The level of entanglement in our distilled state is higher than that achievable by direct transmission of any state through a similar loss channel. This is a key step towards realizing practical continuous-variable quantum communication protocols.

Quantum technology protocols exploit the unique properties of quantum systems to fulfil communication, computing and metrology tasks that are impossible, inefficient or intractable for classical systems[1]. In many cases, the distribution of entanglement, correlations between subsystems that exceed those possible for classical systems, is a necessary condition for quantum technology protocols to succeed. However, entanglement is fragile and can easily be degraded by the communication or storage of the entangled systems. One solution to this problem is entanglement distillation[2]. Given an ensemble of weakly entangled quantum states, distillation techniques allow one to select or distil a smaller sub-ensemble of states that are more strongly entangled. This can be achieved using only local operations and classical communication. In this way, strong entanglement can be established between remote locations under conditions where it would be impossible without distillation (for example, with the losses that are common in quantum communication channels).

There are two broad classes of quantum optical technology protocols: those using quantum observables with a discrete spectrum, such as the spin of an electron, and those using quantum variables with a continuous spectrum, such as the position and momentum of a harmonic oscillator[3]. Our focus here is on the distillation of continuous-variable (CV) states. The primary entangled resource in CV systems is the two-mode squeezed vacuum state, also known as the Einstein–Podolsky–Rosen (EPR) state[4] because its idealized version was introduced by those scientists in the early days of quantum mechanics to illustrate quantum nonlocality.

The EPR state can be used to implement many quantum protocols, including continuous versions of teleportation and quantum key distribution[5]. An advantage of the CV approach to quantum communication is its universality: it is capable of transmitting arbitrary states of light, in contrast to the single-photon subspace of the Hilbert space to which the discrete method is limited. Furthermore, unlike their discrete-variable counterparts, high-quality EPR states are readily available on demand at a high rate from parametric amplifiers.

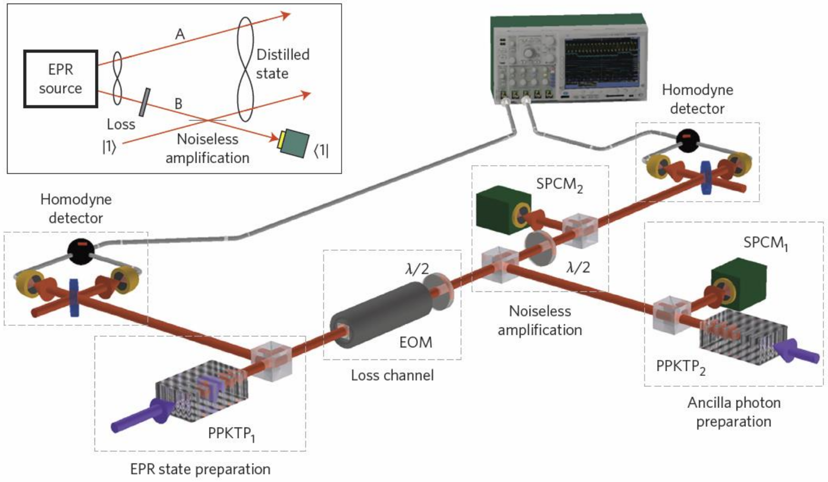
In application to quantum repeaters, those communication protocols that use single photons typically do not need a special distillation procedure to counter the effect of the losses. This is because if a photon is lost, it is not registered by the detector, so a loss event is automatically eliminated from further analysis. In CV protocols, quadrature detection occurs independently of the losses, so recovering an entangled resource suitable for use in a teleportation or repeater protocol requires a dedicated distillation step.

In this Article, we present experimental results demonstrating the distillation of optical CV entanglement in two settings: (1) for very low initial squeezing and (2) after transmission through a lossy channel. In the second setting, we directly observe an entanglement strength of our distilled state that exceeds anything possible via deterministic transmission of the states through the same channel. That is, even if a perfectly pure, infinitely entangled EPR state were passed through that channel, the resulting entanglement would be inferior to what we observe for our distilled state. We will refer to this as breaking the deterministic bound.

Our protocol relies on the technique of noiseless linear amplification (NLA)[6], in contrast to previous CV entanglement distillation demonstrations based on photon subtraction[7,8]. Photon subtraction is unable to enhance entanglement in the EPR state by more than a factor of two, which is by far insufficient to compensate for a loss occurring in a typical communication line. NLA does not suffer from this limitation, and in principle allows the entanglement to be restored to a macroscopic level after an arbitrarily high loss[9]. It is this feature of NLA that enables us to break the deterministic bound. It represents a major step forward in realizing protocols that can enhance quantum technologies under practical conditions.

A key feature of our experiment is that heralded, free-propagating distilled EPR states are produced by our protocol. This differs from a

[1]Russian Quantum Center, 100 Novaya St., Skolkovo, Moscow 143025, Russia. [2]Institute of Fundamental and Frontier Sciences, University of Electronic Science and Technology, Chengdu, Sichuan 610054, China. [3]Moscow Institute of Physics and Technology, Institutsky Lane 9, Dolgoprudny 141700, Russia. [4]P.N. Lebedev Physics Institute, Leninskiy Prospect 53, Moscow 119991, Russia. [5]Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane, Queensland 4072, Australia. [6]Institute for Quantum Science and Technology, University of Calgary, Calgary Alberta T2N 1N4, Canada. [7]Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, Ontario M5G 1Z8, Canada. †These authors contributed equally to this work. *e-mail: lvov@ucalgary.ca



Testing QKD Implementations

RESEARCH ARTICLE

APPLIED MATHEMATICS

Hacking the Bell test using classical light in energy-time entanglement–based quantum key distribution

10.1126/sciadv.1500793

Jonathan Jogenfors,[1]* Ashraf Mohamed Elhassan,[2]* Johan Ahrens,[2] Mohamed Bourennane,[2] Jan-Åke Larsson[1]†

Photonic systems based on energy-time entanglement have been proposed to test local realism using the Bell inequality. A violation of this inequality normally also certifies security of device-independent quantum key distribution (QKD) so that an attacker cannot eavesdrop or control the system. We show how this security test can be circumvented in energy-time entangled systems when using standard avalanche photodetectors, allowing an attacker to compromise the system without leaving a trace. We reach Bell values up to 3.63 at 97.6% faked detector efficiency using tailored pulses of classical light, which exceeds even the quantum prediction. This is the first demonstration of a violation-faking source that gives both tunable violation and high faked detector efficiency. The implications are severe: the standard Clauser-Horne-Shimony-Holt inequality cannot be used to show device-independent security for energy-time entanglement setups based on Franson's configuration. However, device-independent security can be reestablished, and we conclude by listing a number of improved tests and experimental setups that would protect against all current and future attacks of this type.

INTRODUCTION

A Bell experiment (*1*) is a bipartite experiment that can be used to test for preexisting properties that are independent of the measurement choice at each site. Formally speaking, the experiment tests if there is a "local realist" description of the experiment that contains these preexisting properties. Such a test can be used as the basis for security of quantum key distribution (QKD) (*2*, *3*). QKD uses a bipartite quantum system shared between two parties (Alice and Bob) that allows them to secretly share a cryptographic key. The first QKD protocol (BB84) (*2*) is based on quantum uncertainty (*4*) between noncommuting measurements, usually of photon polarization. The Ekert protocol (E91) (*3*) bases security on a Bell test instead of the uncertainty relation. Such a test indicates, through violation of the corresponding Bell inequality, a secure key distribution system. This requires quantum entanglement, and because of this, E91 is also called entanglement-based QKD.

To properly show that an E91 cryptographic system is secure or, alternatively, that no local realist description exists of an experiment, a proper violation of the associated Bell inequality is needed. As soon as a proper violation is achieved, the inner workings of the system is not important anymore, a fact known as device-independent security (*5*, *6*) or a loophole-free test of local realism (*7*). In the security context, the size of the violation is related to the amount of key that can be securely extracted from the system. However, a proper (loophole-free) violation is difficult to achieve. For long-distance experiments, photons are the system of choice and one particularly difficult problem is to detect enough of the photon pairs; this is known as the efficiency loophole (*8*–*10*).

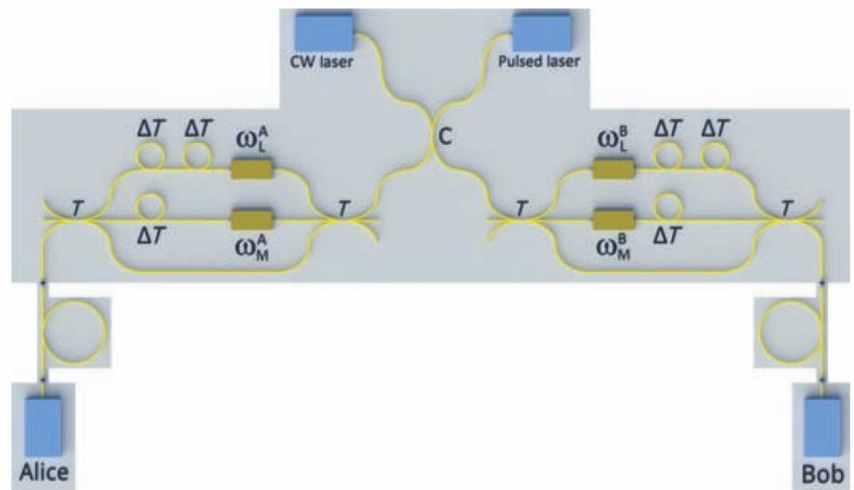
If the violation is not good enough, there may be a local realist description of the experiment, giving an insecure QKD system. Even worse, an attacker could control the QKD system in this case. One particular example of this occurs when using avalanche photodetectors (APDs), which are the most commonly used detectors in commercial QKD systems: these detectors can be controlled by a process called "blinding" (*11*), which enables control via classical light pulses. When using photon polarization in the system, and if the efficiency is low enough in the Bell test, the quantum-mechanical prediction can be faked in such a controlled system (*12*, *13*). This means that the (apparent) Bell inequality violation can be faked, making a QKD system seem secure while it is not. Note that a proper (loophole-free) violation cannot be faked in this manner.

Here, we investigate energy-time entanglement–based systems in general and the Franson interferometer (*14*) in particular. Traditional polarization coding is sensitive to polarization effects caused by optical fibers (*15*), whereas energy-time entanglement is more robust against this type of disturbance. This property has led to an increased attention to systems based on energy-time entanglement because it allows a design without moving mechanical parts, which reduces complexity in practical implementations. A number of applications of energy-time entanglement, such as QKD, quantum teleportation, and quantum repeaters are described by Gisin and Thew (*16*). In particular, Franson-based QKD has been tested experimentally by a number of research groups (*17*–*22*).

It is already known that a proper Bell test is more demanding to achieve in energy-time entanglement systems with postselection (*23*, *24*), but certain assumptions on the properties of photons also reduce the demands to the same level as for a photon polarization–based test (*25*, *26*). The property in question is the particle-like behavior of the photon: it does not "jump" from one arm of an interferometer to the other. Clearly, classical light pulses cannot jump from one arm to the other, so the question arises: Is it at all possible to control the output of the detectors using classical light pulses to make them fake the quantum correlations? Below, we answer this question in the positive and give the details of such an attack and its experimental implementation.

Moreover, not only are faked quantum correlations possible to reach at a faked detector efficiency of 100%, but also, it is even possible to fake the extreme predictions of nonlocal Popescu-Rohrlich (PR) boxes (*27*) at this high detector efficiency. These predictions reach the algebraic

[1]Institutionen för Systemteknik, Linköpings Universitet, 581 83 Linköping, Sweden.
[2]Department of Physics, Stockholm University, 106 91 Stockholm, Sweden.
*These authors contributed equally to this work.
†Corresponding author. E-mail: jan-ake.larsson@liu.se



Troubling Developments In Physics

SCIENCE ADVANCES | RESEARCH ARTICLE

QUANTUM MECHANICS

High-dimensional quantum cloning and applications to quantum hacking

Frédéric Bouchard,[1] Robert Fickler,[1] Robert W. Boyd,[1,2] Ebrahim Karimi[1,3]*

Attempts at cloning a quantum system result in the introduction of imperfections in the state of the copies. This is a consequence of the no-cloning theorem, which is a fundamental law of quantum physics and the backbone of security for quantum communications. Although perfect copies are prohibited, a quantum state may be copied with maximal accuracy via various optimal cloning schemes. Optimal quantum cloning, which lies at the border of the physical limit imposed by the no-signaling theorem and the Heisenberg uncertainty principle, has been experimentally realized for low-dimensional photonic states. However, an increase in the dimensionality of quantum systems is greatly beneficial to quantum computation and communication protocols. Nonetheless, no experimental demonstration of optimal cloning machines has hitherto been shown for high-dimensional quantum systems. We perform optimal cloning of high-dimensional photonic states by means of the symmetrization method. We show the universality of our technique by conducting cloning of numerous arbitrary input states and fully characterize our cloning machine by performing quantum state tomography on cloned photons. In addition, a cloning attack on a Bennett and Brassard (BB84) quantum key distribution protocol is experimentally demonstrated to reveal the robustness of high-dimensional states in quantum cryptography.

INTRODUCTION

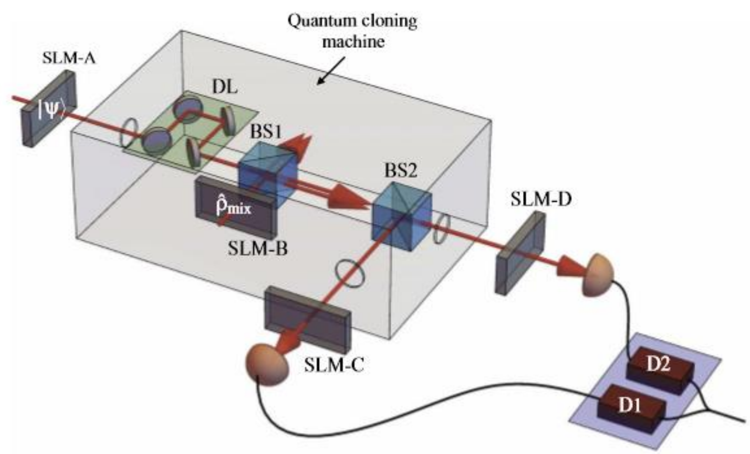
High-dimensional information is a promising field of quantum information science that has matured over the last years. It is known that, by using not only qubits but also qudits, that is, d-dimensional quantum states, it is possible to encode more information on a single carrier, increase noise resistance in quantum cryptography protocols (*1*), and investigate fundamental properties of nature (*2*). Photonic systems have been shown to be promising candidates in quantum computation and cryptography for many proof-of-principle demonstrations as well as for "flying" quantum carriers to distribute high-dimensionally encoded states. Orbital angular momentum (OAM) of light, which provides an unbounded state space, has long been recognized as a potential high-dimensional degree of freedom for conducting experiments on the foundations of quantum mechanics (*3*, *4*), quantum computation (*5*), and cryptography (*6*). The main characteristic of photons carrying OAM is their twisted wavefront, characterized by an $\exp(i\ell\varphi)$ phase term, where ℓ is an integer and φ is the azimuthal coordinate (*7*). In the context of quantum information, OAM states of photons have the advantage of representing quantum states belonging to an infinitely large, but discrete, Hilbert space (*8*). Finite subspaces of dimension d can be considered as laboratory realizations of photonic qudits. Here, we adopt the OAM degree of freedom of single photons to achieve high-dimensional quantum cloning and perform quantum hacking on a high-dimensional quantum communication channel. Although perfect cloning of unknown quantum states is forbidden (*9*), it is interesting to ask how similar to the initial quantum state the best possible quantum clone can be. The answer is given in terms of the cloning fidelity $\mathcal{F}$, which is defined as the overlap between the initial state to be cloned and that of the cloned copies. This figure of merit is a measure of the accuracy of a cloned copy obtained from a specific cloner. Schemes that achieve the best possible fidelity are called optimal quantum cloning and play an important role in quantum information (*10*). For instance, an optimal state estimation yields a bounded fidelity of $\mathcal{F}_{\mathrm{est}} = 2/(1+d)$, where d is the dimension of the quantum state (*11*). Optimal quantum cloning turns out to be a more efficient way of broadcasting the quantum state of a single system because it yields a fidelity that is always higher than that of optimal state estimation, which has been experimentally realized for low-dimensional photonic states (*12*–*15*). Moreover, this enhancement in fidelity grows larger with higher-dimensional quantum states, further motivating experimental investigations of high-dimensional quantum cloning. Hence, high-dimensional optimal quantum cloning machines are of great importance whenever quantum information is to be transmitted among multiple individuals without knowledge of the input quantum state. Here, we concentrate on the $1 \rightarrow 2$ universal optimal quantum cloning machine, for which the optimal fidelity of the two cloned copies is given by $\mathcal{F}_{\mathrm{clo}} = 1/2 + 1/(1+d)$, where d is the dimension of the Hilbert space of the states that are to be cloned (*16*).

RESULTS

Optimal quantum cloning with OAM states of single photons

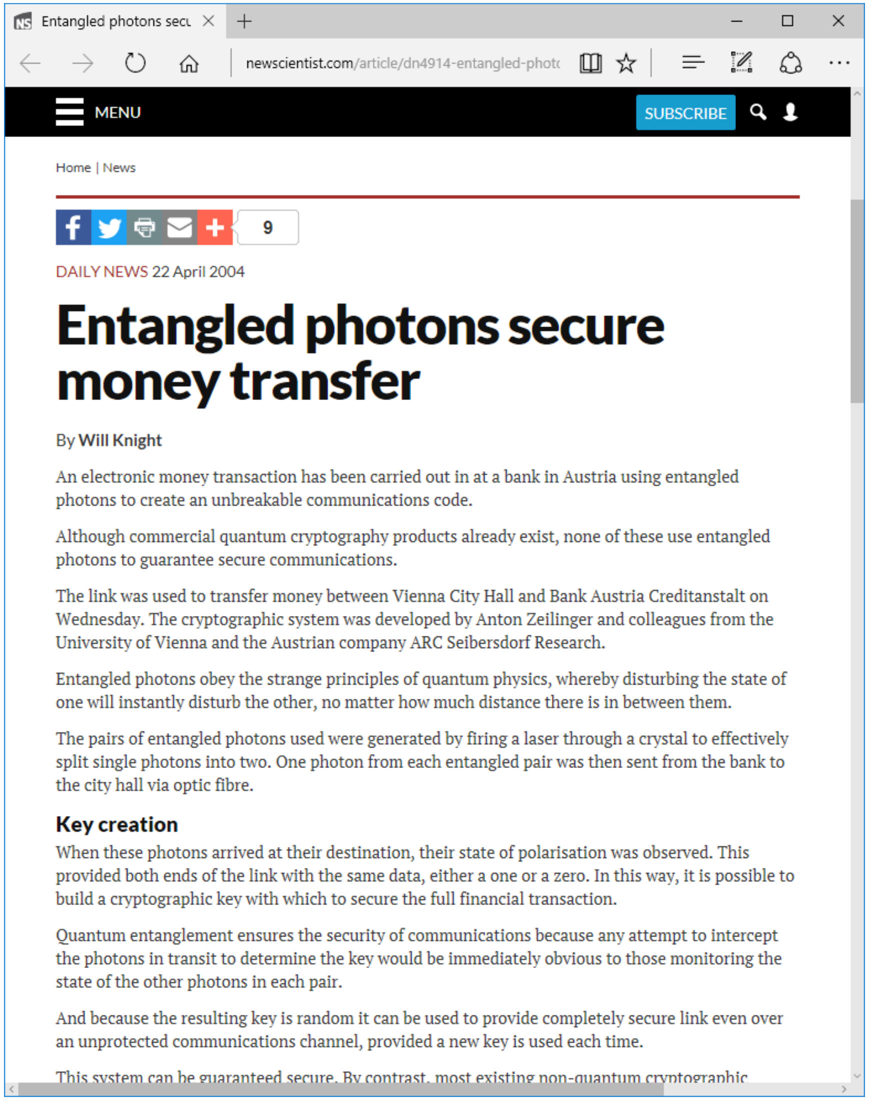
We use the symmetrization method to realize a universal optimal quantum cloning machine for high-dimensional OAM states (*17*, *18*). In this method, the quantum state that is to be cloned, namely, $|\psi\rangle$, is sent to one of the input ports of a nonpolarizing beam splitter. In the other input port, a completely mixed state of the appropriate dimension, given by $\hat{\rho}_{\mathrm{mix}} = I_d/d$, is sent, where I_d is the d-dimensional identity matrix. The symmetrization method relies on the well-known two-photon interference effect at a 50:50 beam splitter first proposed by Hong *et al.* (*19*). When two indistinguishable single photons enter a beam splitter, one into each input port, the photons will "bunch" because of their bosonic nature and exit the beam splitter together through the same output port. This principle is the essence of the symmetrization method for optimal quantum cloning. When both input photons are interfering at the beam splitter, two "cloned" photons will

[1]Department of Physics, University of Ottawa, 25 Templeton Street, Ottawa, Ontario K1N 6N5, Canada. [2]Institute of Optics, University of Rochester, Rochester, NY 14627, USA. [3]Department of Physics, Institute for Advanced Studies in Basic Sciences, 45137-66731 Zanjan, Iran.
*Corresponding author. Email: ekarimi@uottawa.ca



Structure For Talk

- Quantum computers threaten current public key encryption
- Quantum principle behind Quantum Key Distribution
- Quantum Key Distribution in a nutshell
- Is QKD really the answer to the threat posed by quantum computers



Entangled photons secu

newscientist.com/article/dn4914-entangled-phot

MENU

SUBSCRIBE

Home | News

9

DAILY NEWS 22 April 2004

Entangled photons secure money transfer

By Will Knight

An electronic money transaction has been carried out in at a bank in Austria using entangled photons to create an unbreakable communications code.

Although commercial quantum cryptography products already exist, none of these use entangled photons to guarantee secure communications.

The link was used to transfer money between Vienna City Hall and Bank Austria Creditanstalt on Wednesday. The cryptographic system was developed by Anton Zeilinger and colleagues from the University of Vienna and the Austrian company ARC Seibersdorf Research.

Entangled photons obey the strange principles of quantum physics, whereby disturbing the state of one will instantly disturb the other, no matter how much distance there is in between them.

The pairs of entangled photons used were generated by firing a laser through a crystal to effectively split single photons into two. One photon from each entangled pair was then sent from the bank to the city hall via optic fibre.

Key creation

When these photons arrived at their destination, their state of polarisation was observed. This provided both ends of the link with the same data, either a one or a zero. In this way, it is possible to build a cryptographic key with which to secure the full financial transaction.

Quantum entanglement ensures the security of communications because any attempt to intercept the photons in transit to determine the key would be immediately obvious to those monitoring the state of the other photons in each pair.

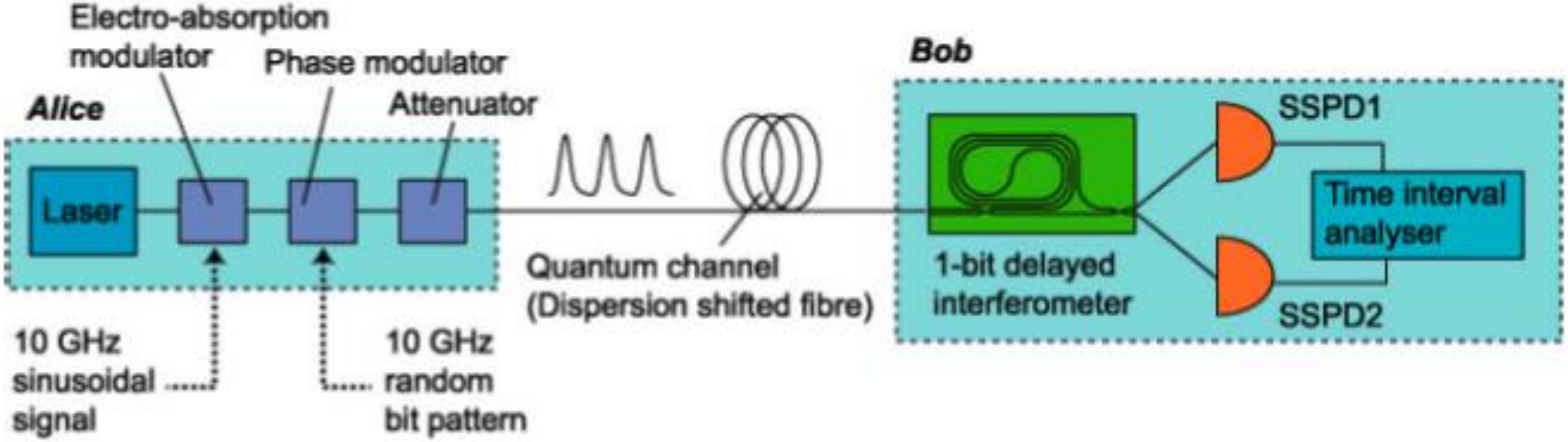
And because the resulting key is random it can be used to provide completely secure link even over an unprotected communications channel, provided a new key is used each time.

This system can be guaranteed secure. By contrast, most existing non-quantum cryptographic

- First used to transfer Euro 3000 between Vienna City Hall and Bank Austria Creditanstalt
- Networks existed since early 2000's but not in common use….yet

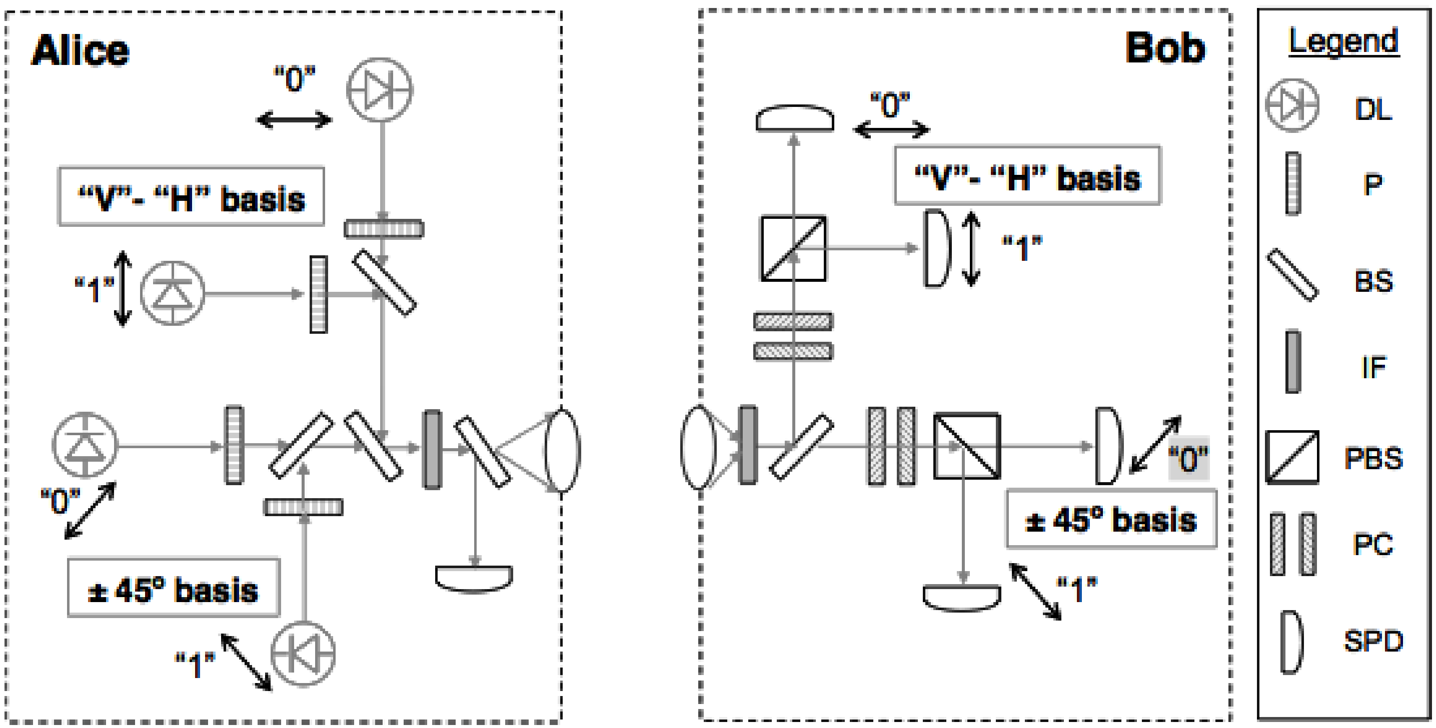
Current State of Affairs

- Current fiber-based distance record: 200 km (Takesue et al)



Current State of Affairs

- Demonstrated free-space link: 10 km



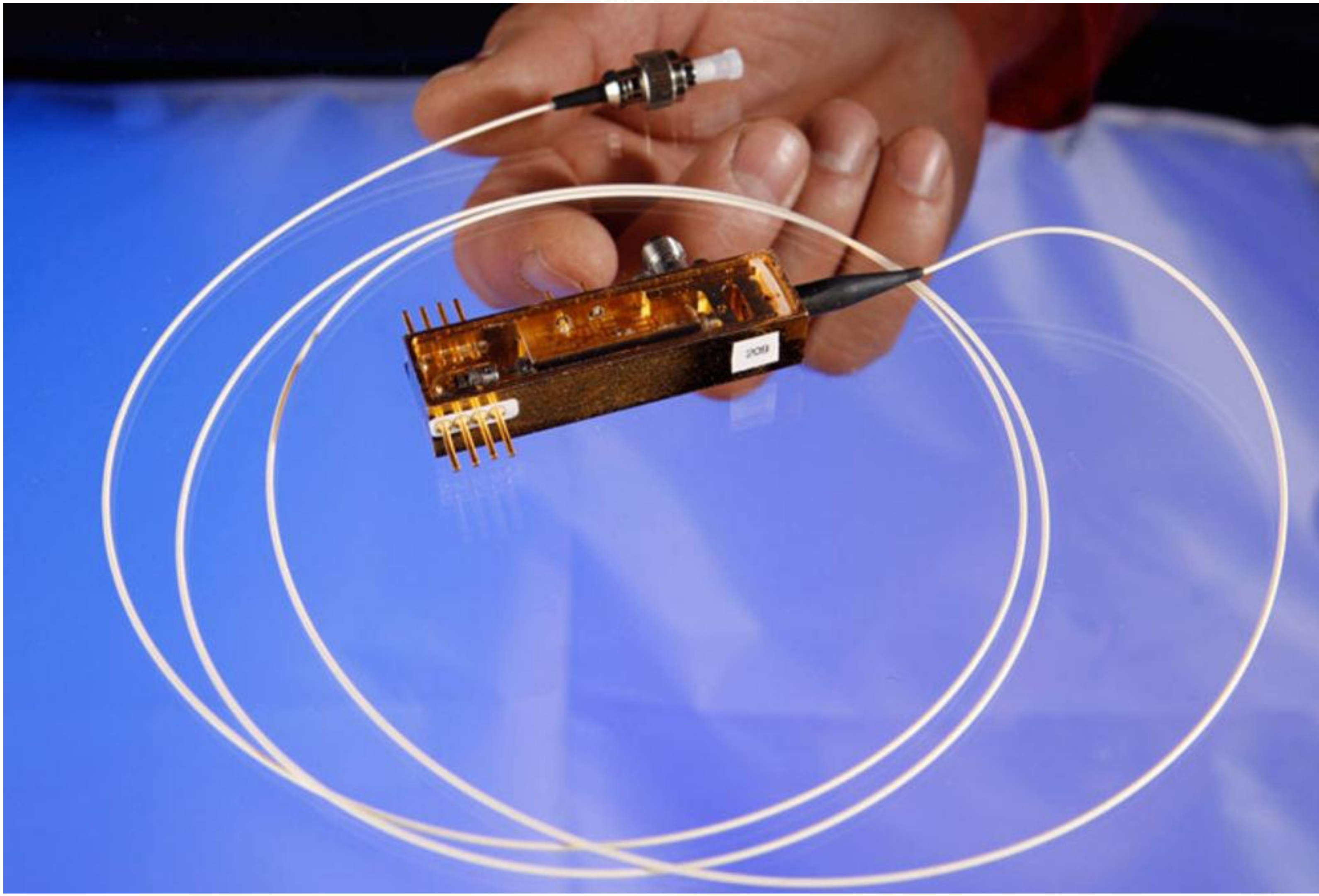
QKD Systems Being Sold Today

Centauris Ethernet Encryption

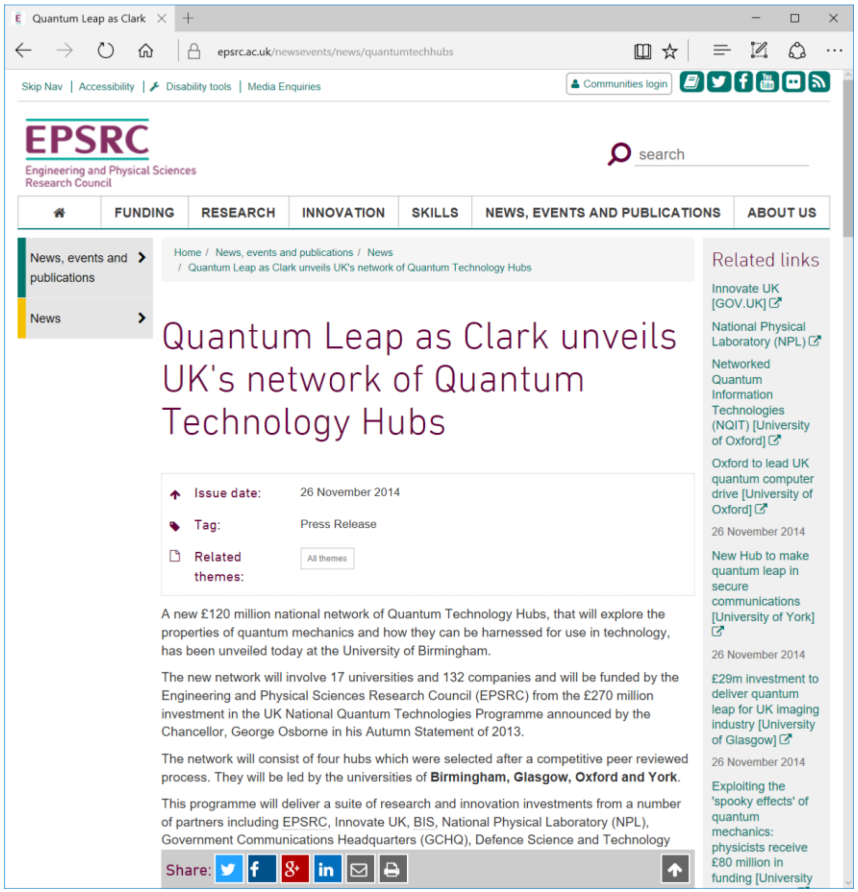
SWISS QUANTUM SECURITY

The Centauris family is a range of quantum-safe high-performance Layer 2 wire-speed encryptors; designed to protect data in-transit from 100Mbps to an aaggregated 100Gbps. The encryptors integrate transparently and simply into existing networks and can be upgraded to quantum cryptography through the addition of the Cerberis QKD Server for long term data protection.

Los Alamos Experiments Show Miniaturization



UK Govt Has A Plan - £270m



Quantum Leap as Clark

epsrc.ac.uk/newsevents/news/quantumtechhubs

Skip Nav | Accessibility | Disability tools | Media Enquiries

Communities login

EPSRC
Engineering and Physical Sciences Research Council

search

FUNDING | RESEARCH | INNOVATION | SKILLS | NEWS, EVENTS AND PUBLICATIONS | ABOUT US

News, events and publications

News

Home / News, events and publications / News / Quantum Leap as Clark unveils UK's network of Quantum Technology Hubs

Quantum Leap as Clark unveils UK's network of Quantum Technology Hubs

Issue date: 26 November 2014

Tag: Press Release

Related themes: All themes

A new £120 million national network of Quantum Technology Hubs, that will explore the properties of quantum mechanics and how they can be harnessed for use in technology, has been unveiled today at the University of Birmingham.

The new network will involve 17 universities and 132 companies and will be funded by the Engineering and Physical Sciences Research Council (EPSRC) from the £270 million investment in the UK National Quantum Technologies Programme announced by the Chancellor, George Osborne in his Autumn Statement of 2013.

The network will consist of four hubs which were selected after a competitive peer reviewed process. They will be led by the universities of **Birmingham, Glasgow, Oxford and York**.

This programme will deliver a suite of research and innovation investments from a number of partners including EPSRC, Innovate UK, BIS, National Physical Laboratory (NPL), Government Communications Headquarters (GCHQ), Defence Science and Technology

Share:

Related links

Innovate UK [GOV.UK]

National Physical Laboratory (NPL)

Networked Quantum Information Technologies (NQIT) [University of Oxford]

Oxford to lead UK quantum computer drive [University of Oxford]

26 November 2014

New Hub to make quantum leap in secure communications [University of York]

26 November 2014

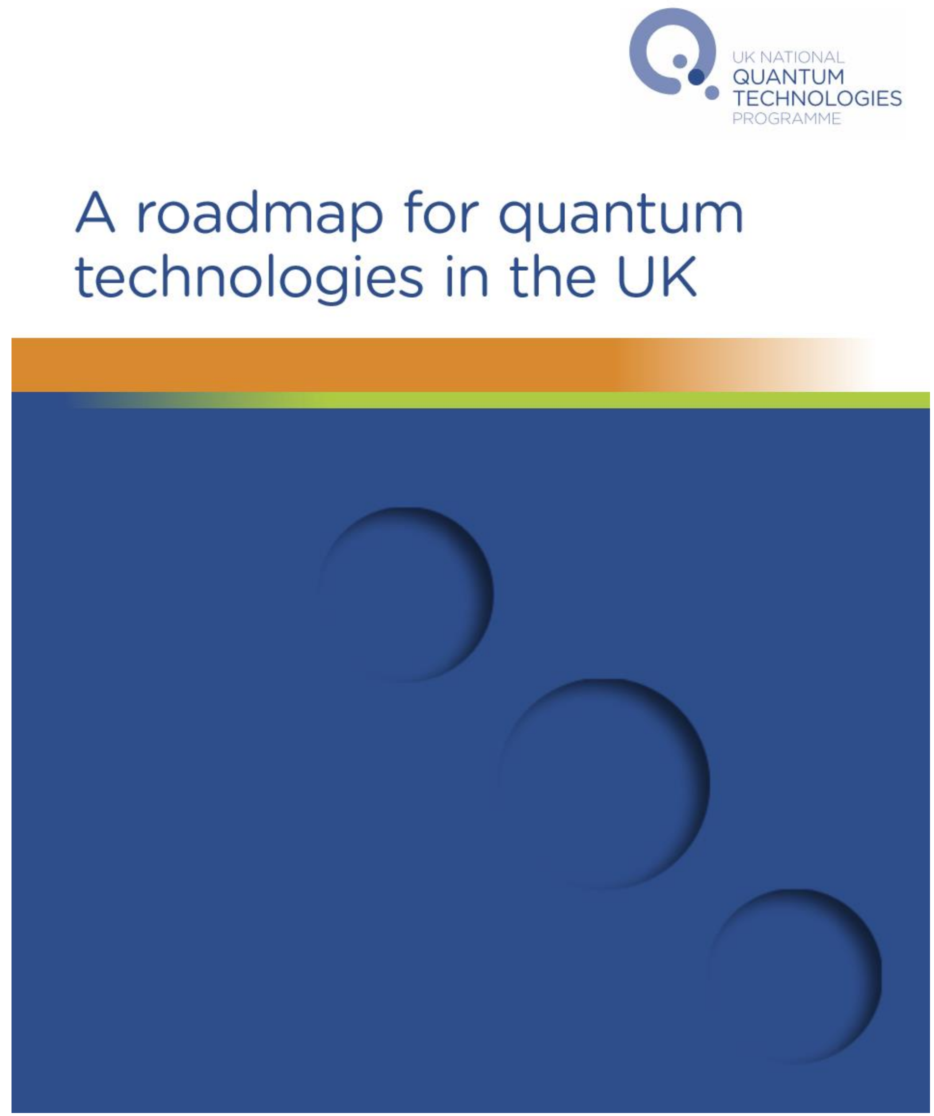
£29m investment to deliver quantum leap for UK imaging industry [University of Glasgow]

26 November 2014

Exploiting the 'spooky effects' of quantum mechanics: physicists receive £80 million in funding [University

KTN the Knowledge Transfer Network

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME



UK Quantum Technology Hub

QUANTUM COMMUNICATIONS HUB

Members login

About us | People | Industrial Engagement | Partnership Resource | Partners | Vacancies | News & Events | Resources | Contact Us

Quantum Communications Hub

UK Quantum Technology Hub for Quantum Communications Technologies

The UK Quantum Technology Hub for Quantum Communications is a synergistic partnership of eight UK Universities (Bristol, Cambridge, Heriot-Watt, Leeds, Royal Holloway, Sheffield, Strathclyde, and York), numerous private sector companies (BT, the National Physical Laboratory, Toshiba Research Europe Ltd, amongst others), and public sector bodies (Bristol City Council and the National Dark Fibre Infrastructure Service), that have come together in a unique collaboration to exploit fundamental laws of quantum physics for the development of secure communications technologies and services.

Led by the University of York, the five-year, £24m QComm Hub aims to deliver quantum encryption systems that will in turn enable secure transactions and transmissions of data across a range of users in real-world applications: from government agencies and industrial set-ups to commercial establishments and the wider public. The project is part of a major national initiative, the UK National Quantum Technologies Programme, which aims to ensure the successful transition of quantum technologies from laboratory to industries.

QUANTIC

Visit QuantIC Hub website

NQIT Networked Quantum Information Technologies

Visit NQIT Hub website

ADVA Optical Networking

AIRBUS DEFENCE & SPACE

University of BRISTOL

BRISTOL CITY COUNCIL

BT

UNIVERSITY OF CAMBRIDGE

Cambridge Network

CESG
The Information Security Arm of GCHQ

ETSI

HERIOT WATT UNIVERSITY

IDQ
FROM VISION TO TECHNOLOGY

UNIVERSITY OF LEEDS

NPL
National Physical Laboratory

NDFIS
National Dark Fibre Infrastructure Service

OCLARO

ROYAL HOLLOWAY UNIVERSITY OF LONDON

The University Of Sheffield.

University of Strathclyde Glasgow

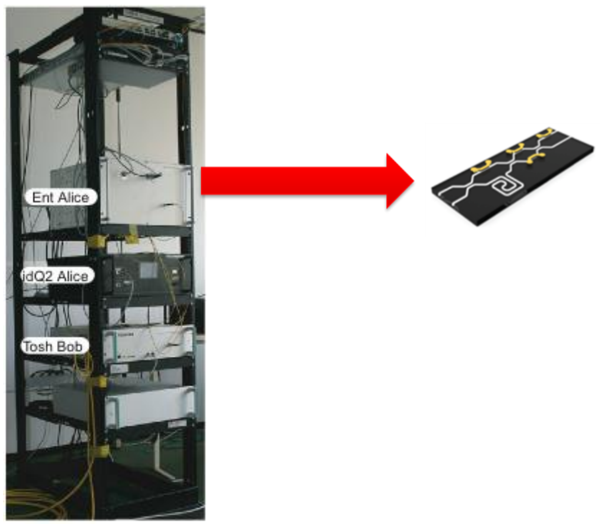
TOSHIBA
Leading Innovation >>>

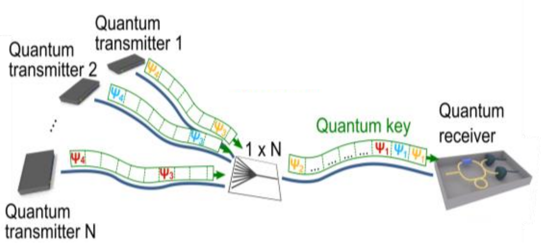
L3 TRL Technology
one step ahead

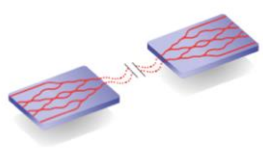
UNIVERSITY of York

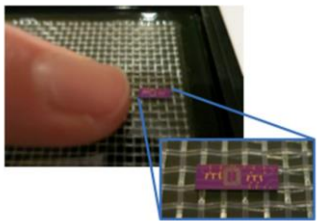
Chip-based QKD modules

- Chip-based modules offer:
  - Low cost; compact size, energy efficiency; mass manufacture capability; compatibility with current microelectronics…
- All these features open up wider applications and markets





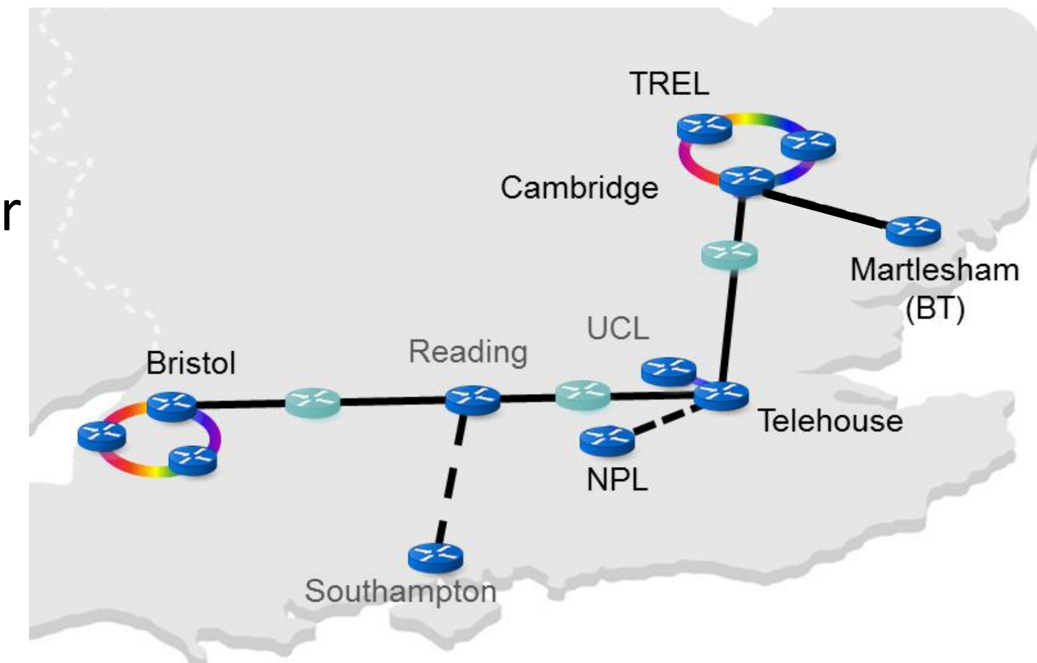




UK Quantum Network (UKQN)

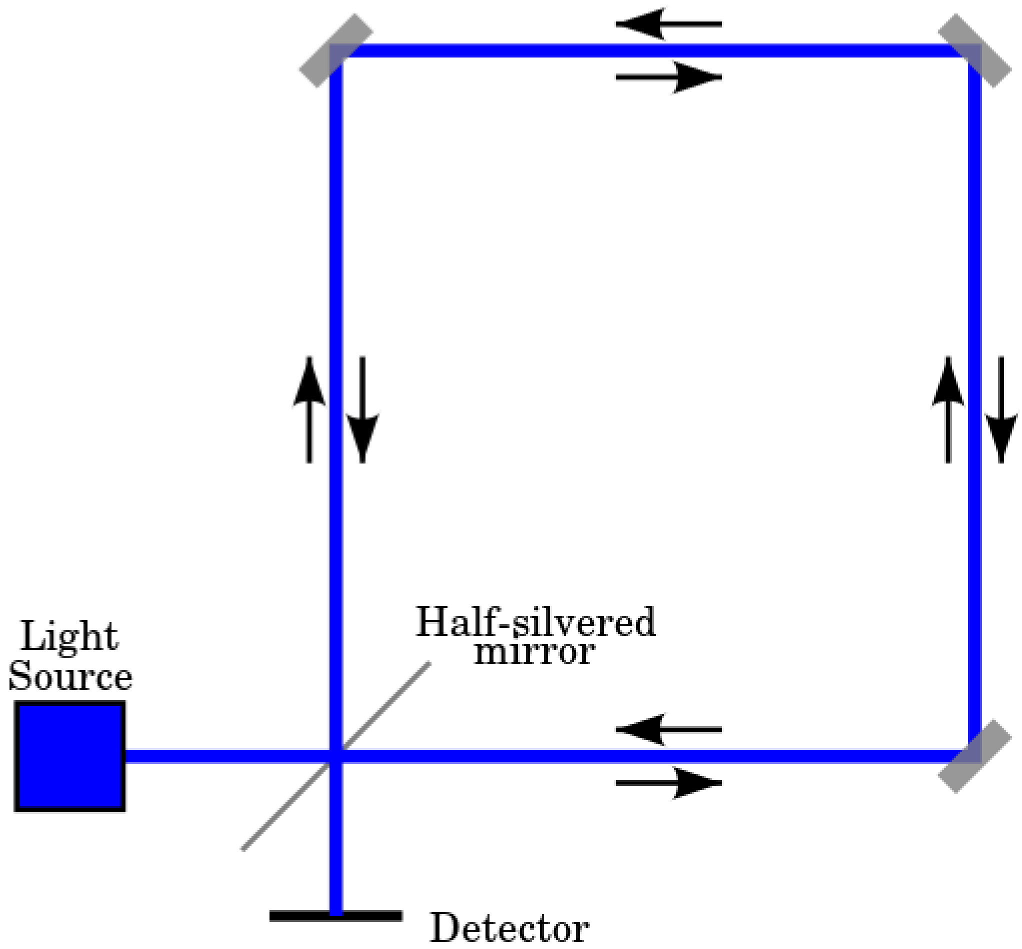
- A focus for development of new applications and standards, user-engagement and market generation
- A showcase for new quantum technologies

- Metro networks in Bristol and Cambridge
- Access networks for multi-user scenarios
- Recent ADVA, BT and Toshiba demonstration of 200G over 100km

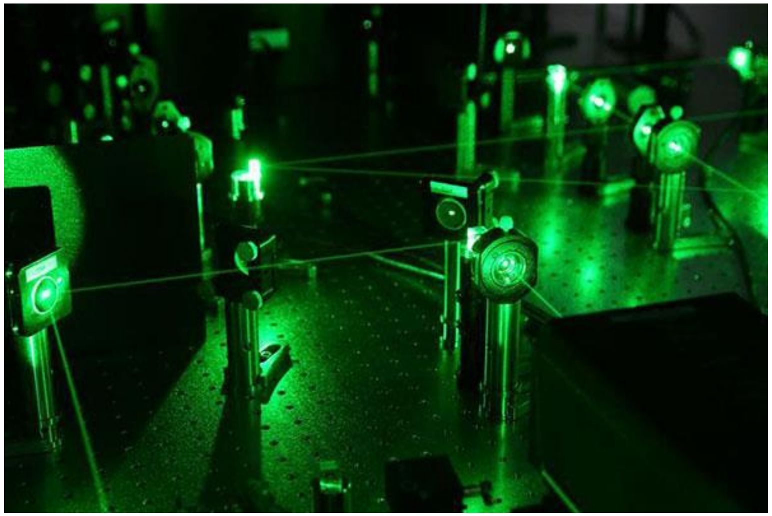


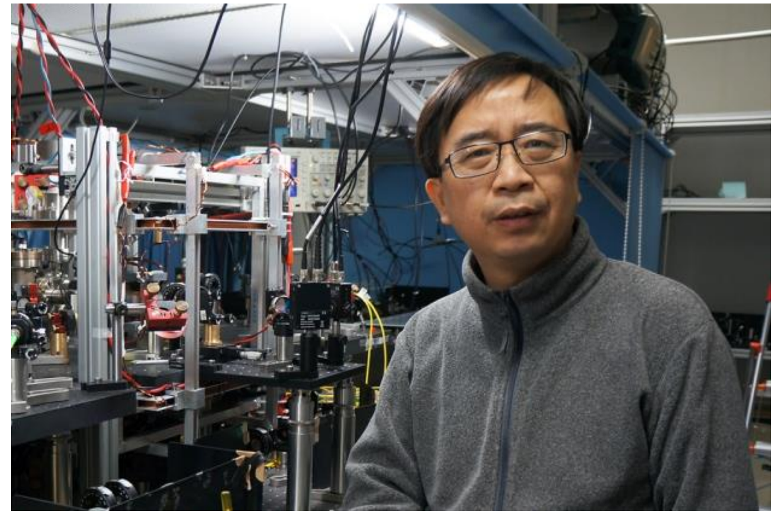
Chinese Entangled Photon Satellite: Micius

Sagnac Effect Interferometer: Original Idea For Entangled Photons



Entanglement Source In Micius



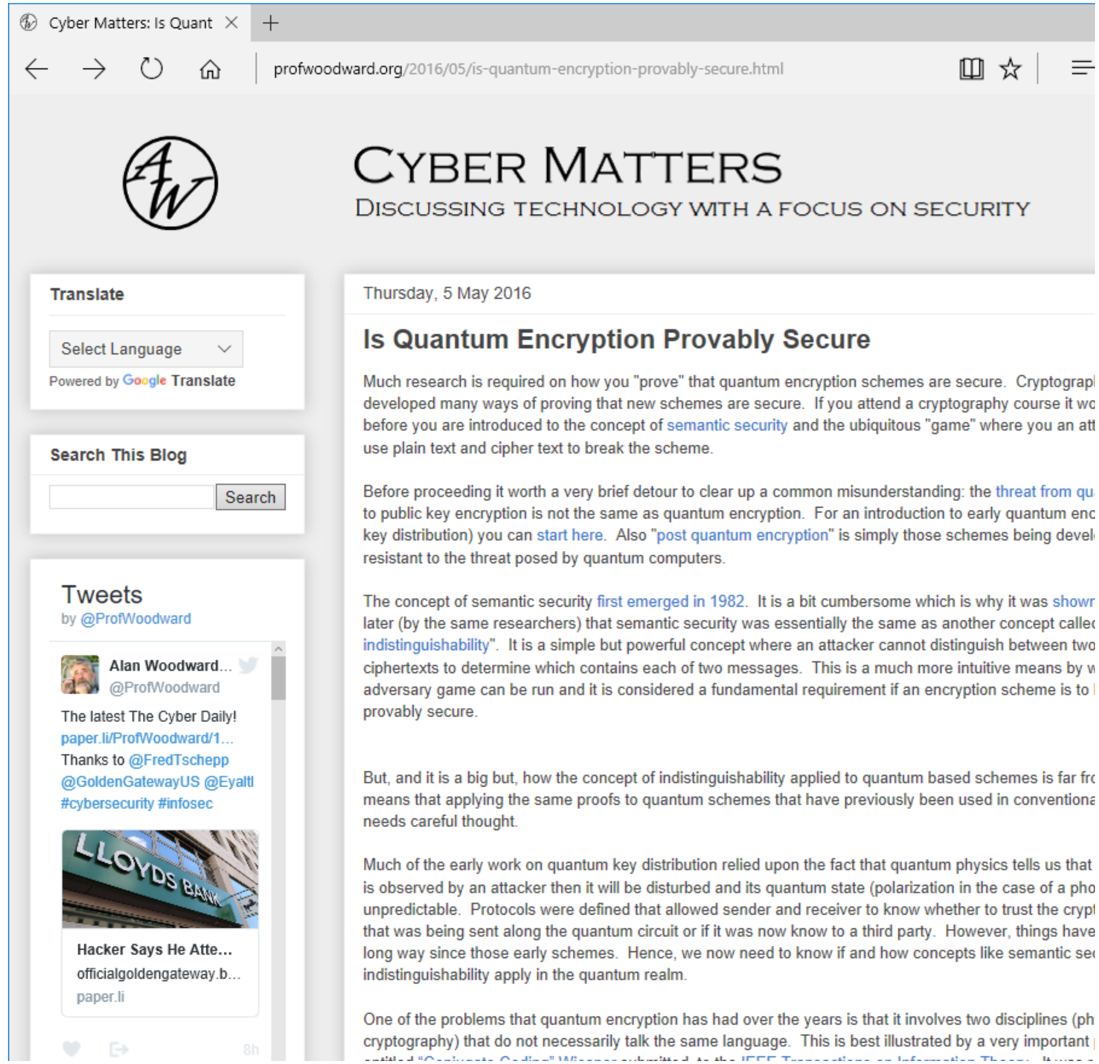


Receiving Stations:
China & Austria

Security proofs

- Mayers, 1998.
- Lo, Chau, 1999.
- Preskill, Shor, 2000.
- Boykin et.al., 2000.
- Ben-Or, 2000.

Much talk about "unconditional security"



“Unconditional Security” (1)

- Many papers talk (and “prove”) that QKD provides “unconditional security” but…
- Cryptographers & physicists mean rather different things by this term
- Physicists mean that the quantum channel cannot be intercepted without it being detected – this you can prove
- Cryptographers (who also talk about “perfect secrecy”) mean:
- No matter the computational power & time available a secret cannot be discovered
- Integrity & Authentication can be proven as well as Confidentiality

“Unconditional Security” (2)

- QKD as BB84 (& variants) has a public channel so this would require a Message Authentication Code (MAC) if the protocol as a whole were to be unconditionally secure:
  - To secure the public channel requires some form of public key crypto even for a simple MAC which rather defeats the object of QKD replacing PKI
- QKD bit rate is relatively slow so (as per Shannon) you need a key same length as message for unconditional security so it limits message speeds
- Should we ne talking about QKD in terms of “computational security” or “provable security” ie with limited computational power & time recovering secret is infeasible
- Some cryptographers argue that QKD (certainly in the from of BB84 etc) cannot be considered a replacement for current public key crypto & that QKD is really more of a symmetric encryption primitive

RANDOM.ORG

Google™ Custor

True Random Number Service

Do you own an iOS or Android device? Check out our app!

What's this fuss about *true* randomness?

Perhaps you have wondered how predictable machines like computers can generate randomness. In reality, most random numbers used in computer programs are *pseudo-random*, which means they are generated in a predictable fashion using a mathematical formula. This is fine for many purposes, but it may not be random in the way you expect if you're used to dice rolls and lottery drawings.

RANDOM.ORG offers *true* random numbers to anyone on the Internet. The randomness comes from atmospheric noise, which for many purposes is better than the pseudo-random number algorithms typically used in computer programs. People use RANDOM.ORG for holding dra
sweepstakes, to drive online games, for scientific applications and for art and r
existed since 1998 and was built by Dr Mads Haahr of the School of Computer
Trinity College, Dublin in Ireland. Today, RANDOM.ORG is operated by Randon
Services Ltd.

As of today, RANDOM.ORG has generated 1.43 trillion random bits for the Inte

True Random Number Generator

Min: 1

Max: 100

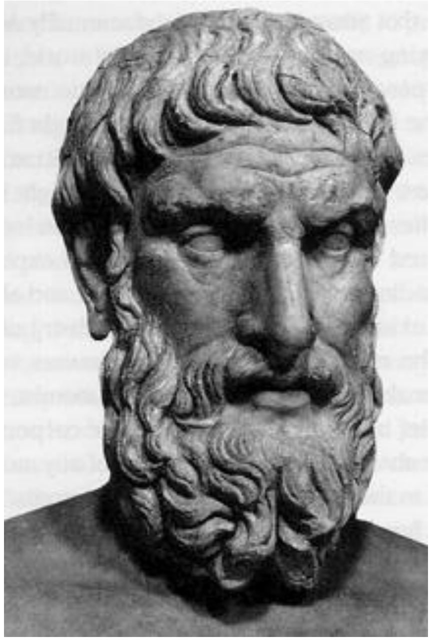
Generate

Result:

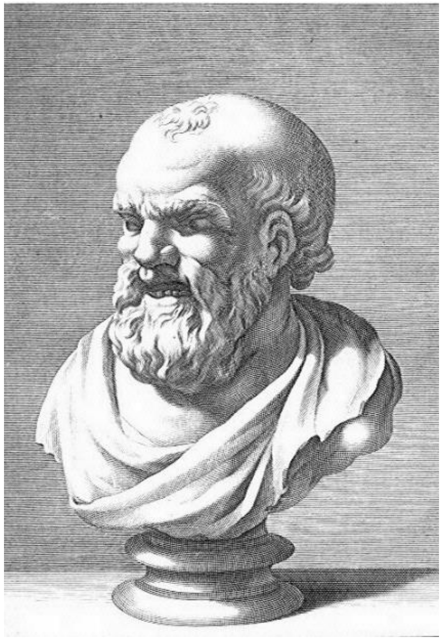
But What If.....

- Quantum channel could:
  - Share a truly random sequence
  - Guarantee that no one else knew the sequence
  - Could communicate the sequence as an ongoing stream equal to the message length at practical rate
- Do we have the basis of a quantum One Time Pad
  - The OTP is the only known truly “unconditionally” secure scheme
- Opens up questions about what is “random”
  - If everything is quantum is anything really random
- Ekert has proposed just such a device independent approach!

Beyond the simplistic mathematical model



If everything is quantum
then
what is randomness?



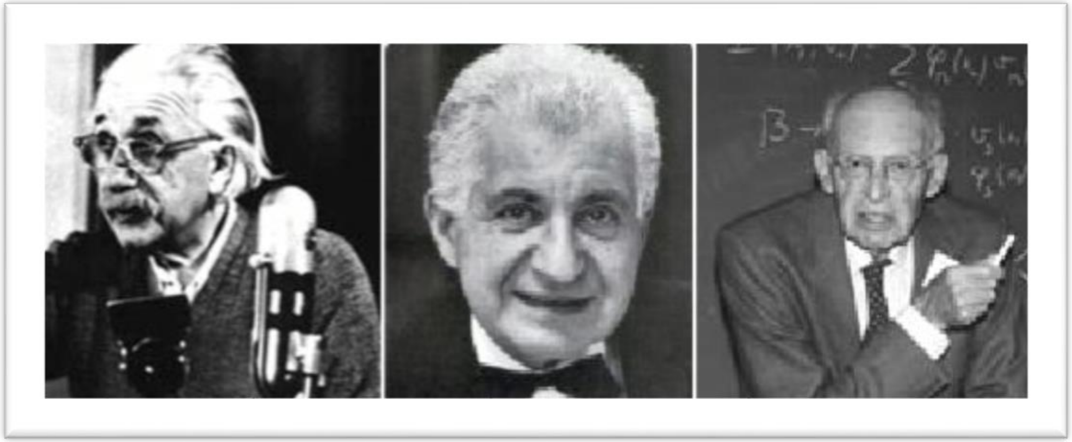
EPICURUS
(300 BC)

OBJECTIVE

DEMOCRITUS
(400 BC)

SUBJECTIVE

Many open questions



Einstein Podolsky Rosen

EPR vision of reality is too simplistic

Hugh Everett

Security and Randomness
in the multiverse

So Is QKD The Answer To Shor's Algorithm?

- Many hail QKD as the answer to quantum computing & Shor's algorithm – especially those selling the products
- It has limitations:
  - Cost: expensive hardware infrastructure required
  - Point to point: although this is possible down to domestic level with infrastructure
  - Limited distance before repeaters required: weaknesses in the chain
- Implementation issues mean it is not as secure as the ideal case suggests
- Ekert 91 based satellite model could be a generalised secure key sharing scheme available to all
- Ekert still not used commercially – commercial systems use BB84 or variants:
  - "There is still a way to go before it becomes a standard commercial proposition, but we are getting there faster than I expected," Artur Ekert, but
  - Chinese pushing hard but so far achieved relatively low bandwidths
- Commercialisation is overwhelmingly using BB84 or variants but…
- Protocols such as BB84 are not "unconditionally secure" so is it better to find a "Quantum Resistant" encryption scheme that can replace RSA & Elliptic Curve based systems eg Ring LWE?

UK’s NCSC Advice On QKD

Direction

For all the practical, business and security reasons given above, at this point in time we:

- do not endorse QKD for any government or military applications
- advise against replacing any existing public key solutions with QKD for commercial applications

The UK should continue its research and development of QKD systems. But this should be balanced by a growing body of practical QKD vulnerability research, and accompanied by the development of methods for quantifying and validating the security claims of real-world QKD systems. Responsible innovation should be accompanied by independent validation.

Our advice is unlikely to change until:

- commercial standards for QKD have been established, building on the experience gained from practical vulnerability research and incorporating quantifiable security validation methods
- the full life cycle support costs for commercial QKD systems are much better understood

We encourage research into developing post-quantum public key cryptography as a more practical and cost-effective step towards defending real-world communications systems against the threat of a future quantum computer.

We do not see the need to upgrade current systems as urgent, though a transition to post-quantum public key cryptography will be necessary. A steady and considered upgrade process will allow time for researchers to reach a consensus as to the best postquantum protocols for various applications.

Summary

QKD:

- has fundamental practical limitations
- does not address large parts of the security problem
- is poorly understood in terms of potential attacks

By contrast, post-quantum public key cryptography appears to offer much more effective mitigations for real-world communications systems from the threat of future quantum computers.

Can QKD Counter The Threat Posed by Quantum Computers To Public Key Encryption?

Cryptographers' answer: Not unconditionally secure so why is it any better than post quantum candidates. Not really a substitute for PKI

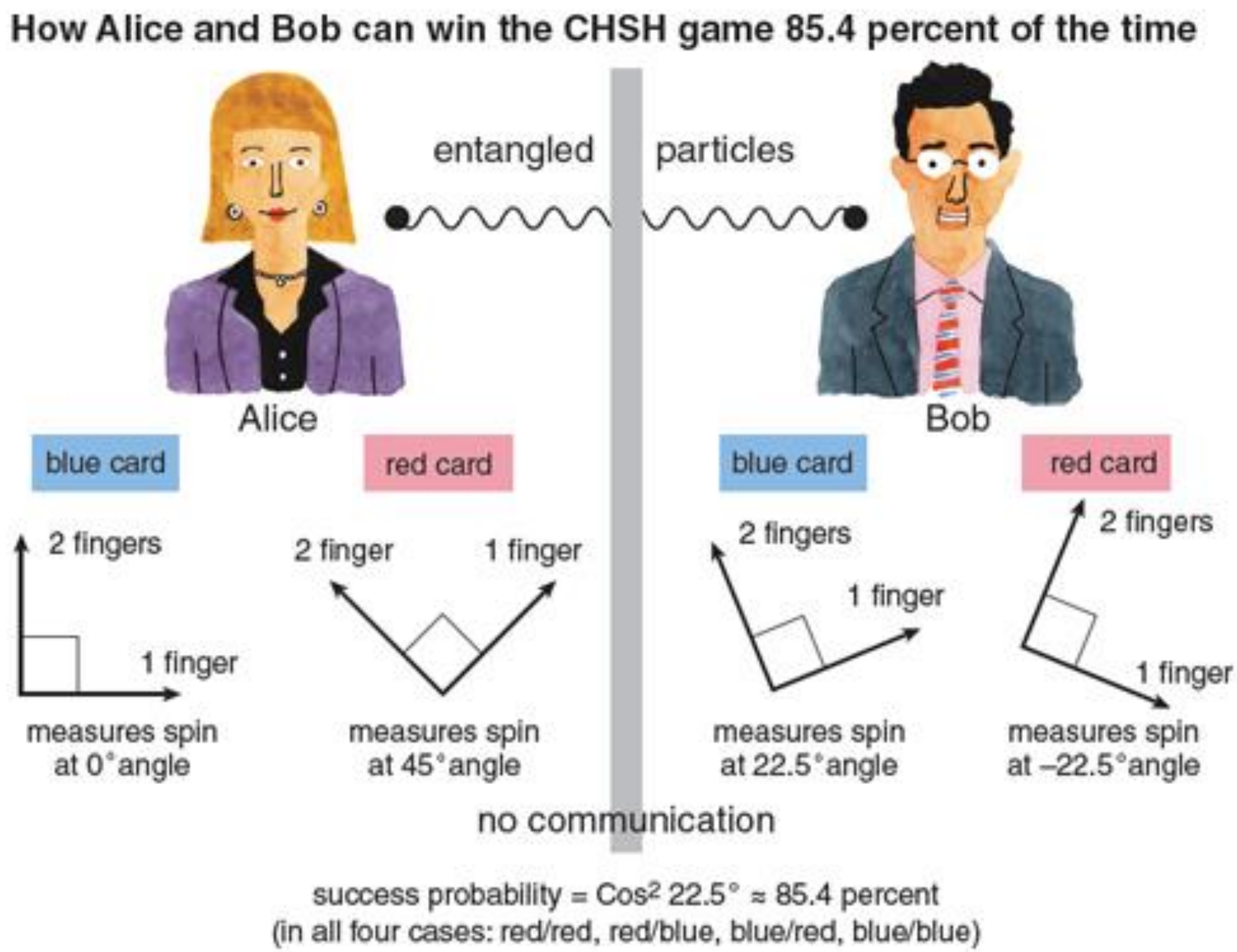
Physicists' answer: Probably but not necessarily using BB84

Engineers' answer: Let's try it & see

Any Questions?

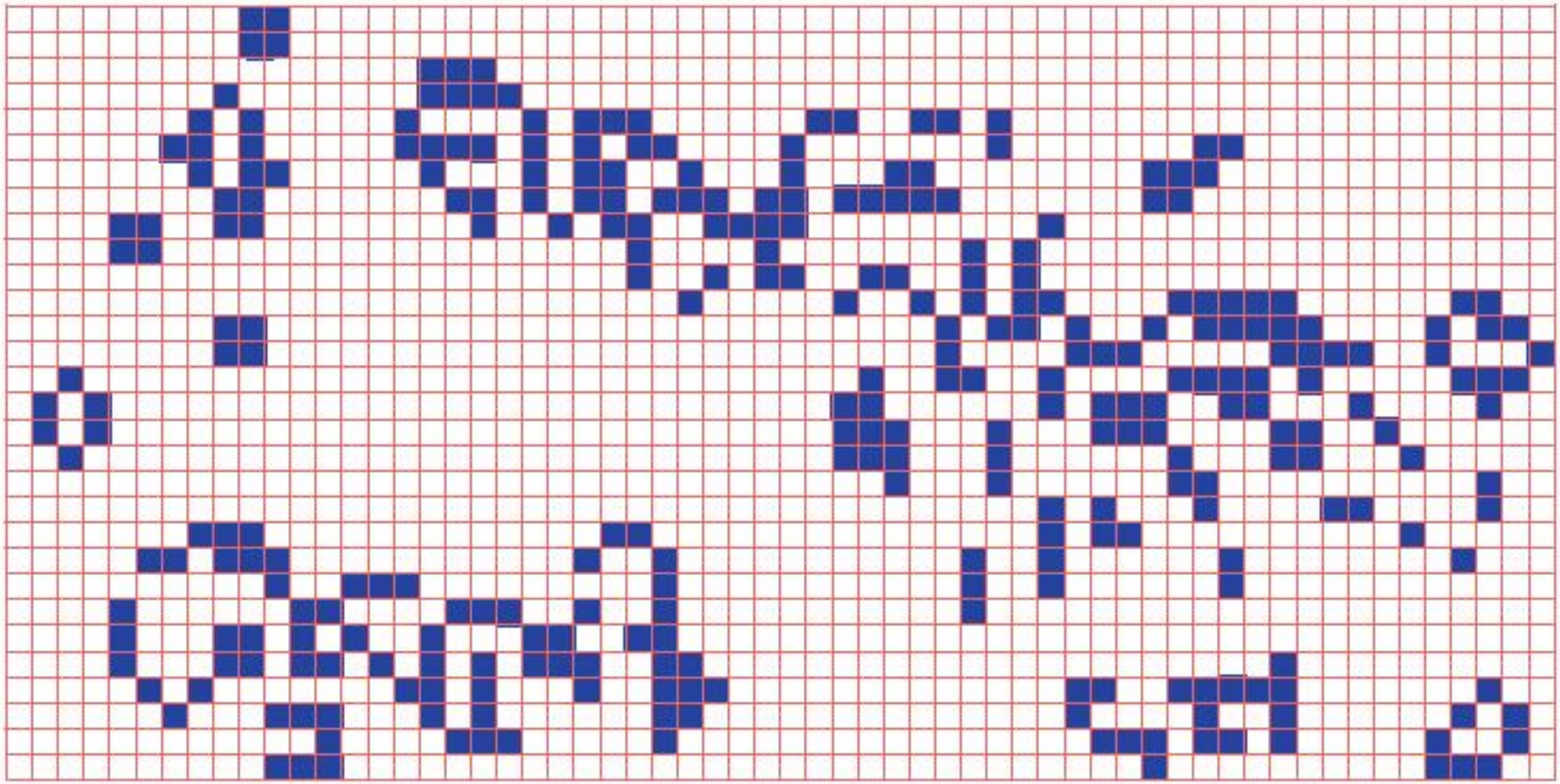
"About your cat, Mr. Schrödinger—I have good news and bad news."

Game By Clauser, Horne, Shimony & Holt



probabilities (percentages)					
card colors	number of fingers raised by Alice, Bob				Alice and Bob win
	1,1	**1,2**	**2,1**	**2,2**	
blue/blue	42.7	7.3	7.3	42.7	probability (1,1) + probability (2,2) = 85.4
blue/red	42.7	7.3	7.3	42.7	probability (1,1) + probability (2,2) = 85.4
red/blue	42.7	7.3	7.3	42.7	probability (1,1) + probability (2,2) = 85.4
red/red	7.3	42.7	42.7	7.3	probability (1,2) + probability (2,1) = 85.4

Conway's Game Of Life



Coudron-Yuen Randomness Laundering