量子暗号


NUS
National University of Singapore
GSIS
Graduate School of Information Sciences.
TOHOKU University
東北大学　情報科学研究科
CQT, シンガポール国立大学
林　正人
東北大学 大学院情報科学研究科
Graduate School of Information Sciences.TOHOKU University
DEX-SMI
TOHOKU
UNIVERSITY
CQT
Centre for
Quantum
Technologies

内容

- 量子暗号の基礎
- 盗聴対策技術：秘匿性増強
- 量子暗号の将来

シャノンの使い捨て暗号

Alice

Bob

暗号化

解読

メッセージ

共有秘密鍵

暗号文

共有秘密鍵

復号文

$$Z_1 \quad X_1 \quad Y_1 = X_1 + Z_1 \quad X_1 \quad X_1 + Y_1 = Z_1$$

$$Z_2 \quad X_2 \quad Y_2 = X_2 + Z_2 \quad X_2 \quad X_2 + Y_2 = Z_3$$

$$Z_3 \quad X_3 \quad Y_3 = X_3 + Z_3 \quad X_3 \quad X_3 + Y_3 = Z_3$$

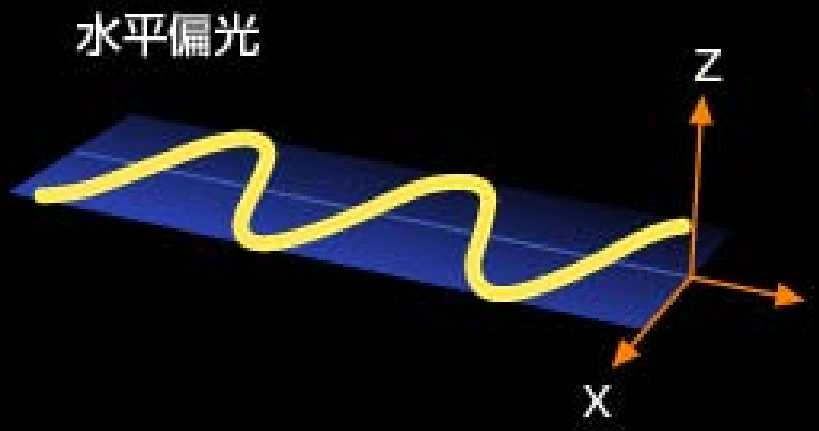
$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$

ただし、ここでは排他的論理和(XOR,1+1=0）

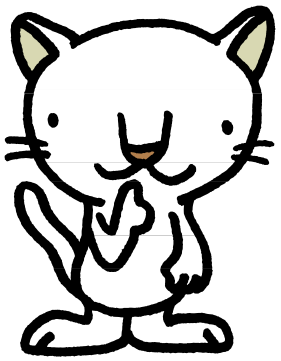
メッセージと同じ桁数の
秘密の同じ乱数があればOK！

でも、どうやって
秘密の同じ乱数を準備するの？

量子暗号を用いれば可能！



量子暗号ってなに？



- 光の偏光などの量子を用いて、秘密の乱数（秘密鍵）を配るシステム
- 光を弱くすることで、実現が可能.

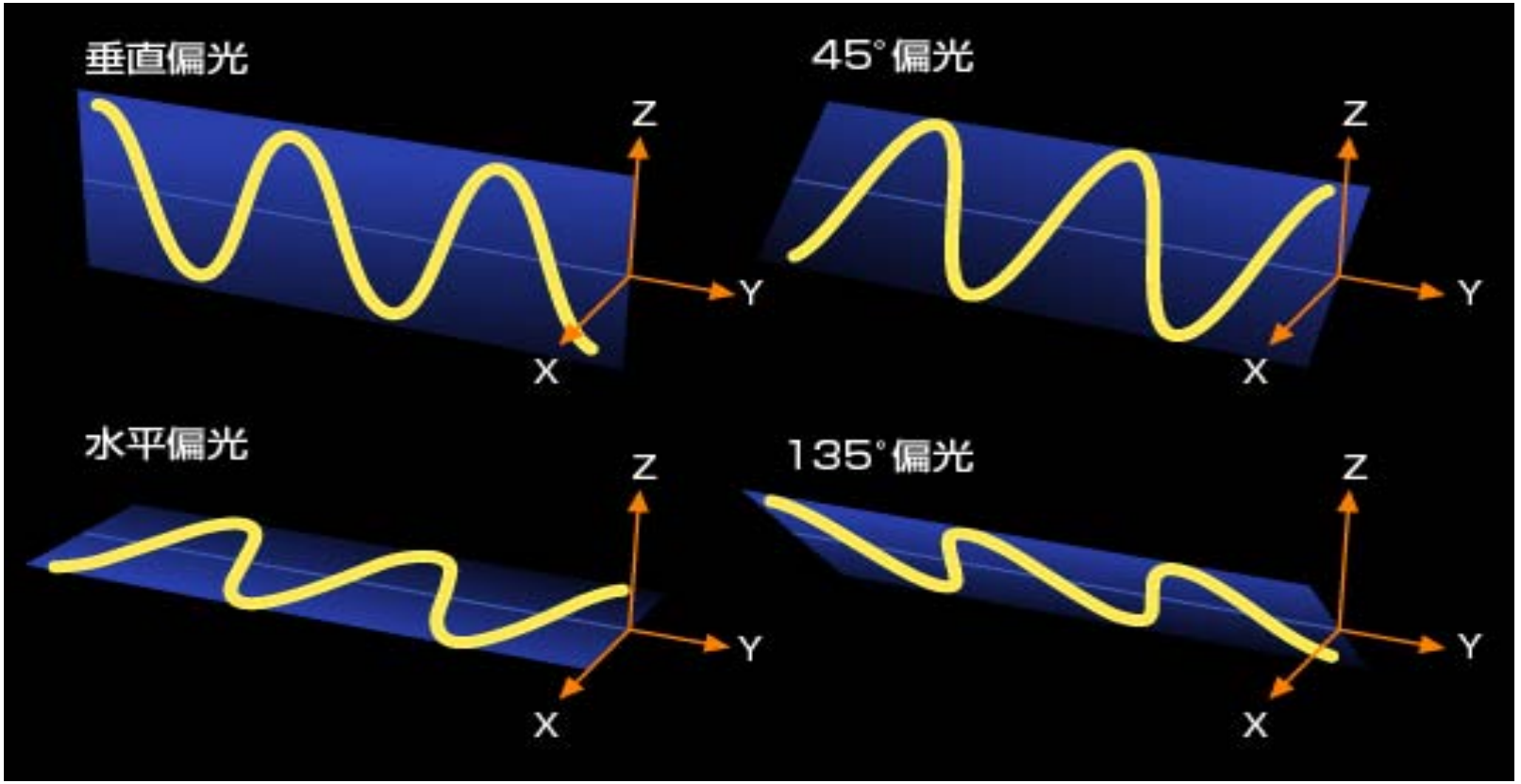
量子ってなに？

- ナノの世界よりも、もっと小さい世界。
- 物質は何でも非常に小さく（弱く）すると粒子と波の両方の性質が現れる！
- 光を弱くすると、光の粒子（光子または量子）になる.

暗室の中

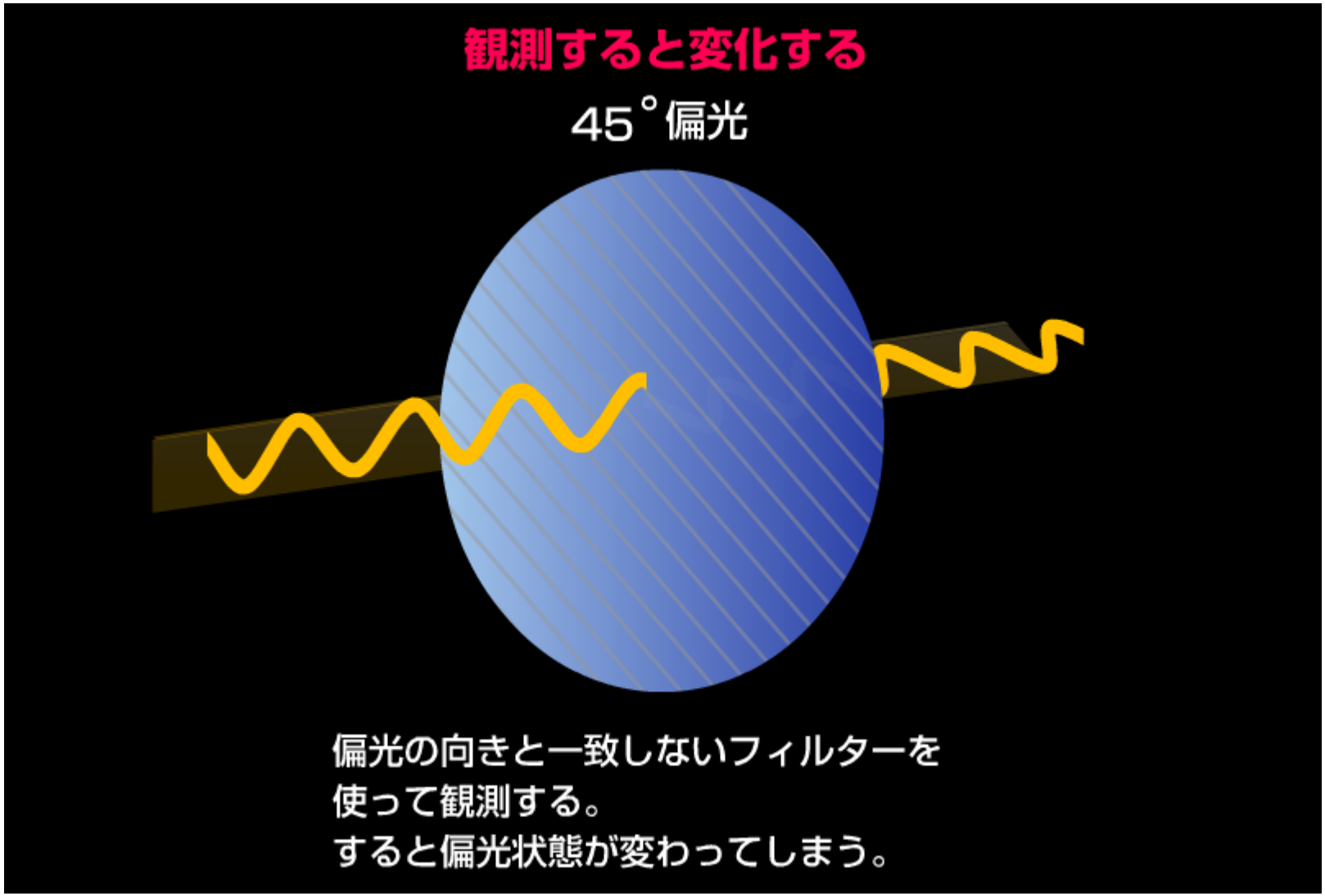
量子ってなに？

- 光は波なので、光子は波の向きである偏光を持っている。
  波長　赤: 700nm，緑: 546.1nm，青: 435.8nm



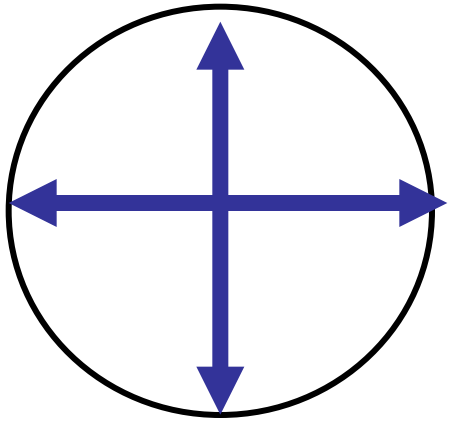
ニコン「光と人の物語」破られない暗号（横山広美著，今井浩・林正人監修）より
http://www.nikon.co.jp/main/jpn/feelnikon/discovery/light/chap04/sec01.htm

偏光は観測すると変化するよ！



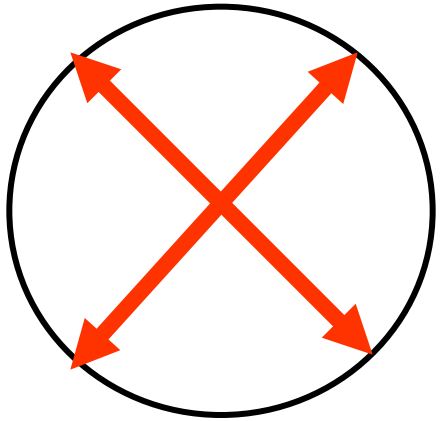
ニコン「光と人の物語」破られない暗号（横山広美著，今井浩・林正人監修）より
http://www.nikon.co.jp/main/jpn/feelnikon/discovery/light/chap04/sec01.htm

直交する偏光の向きは偏光板で識別できる！



垂直偏光と水平偏光

＋基底



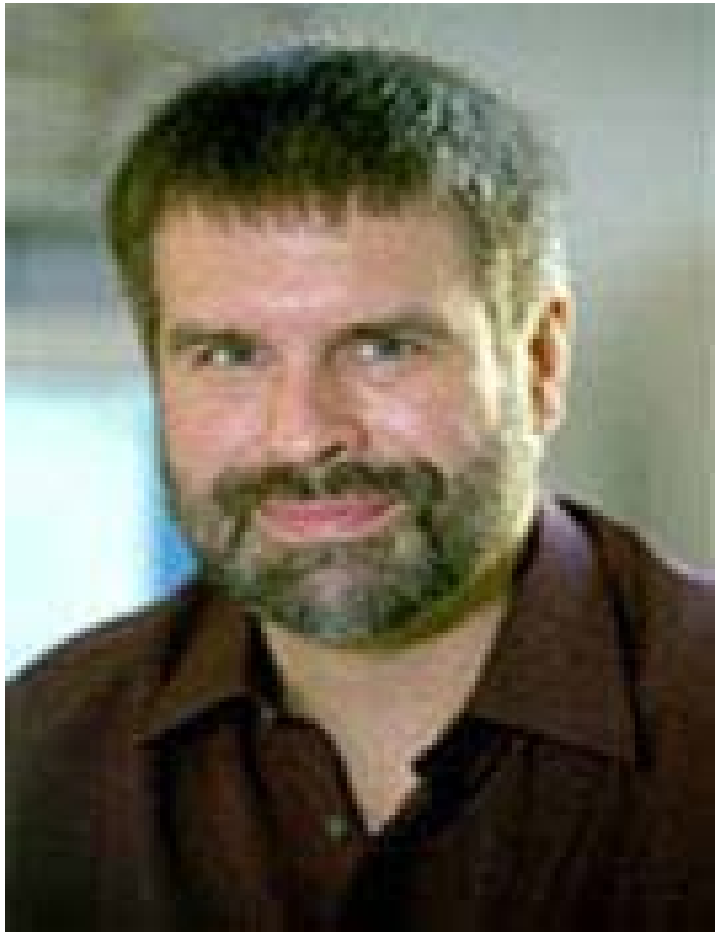
45°偏光と135°偏光

×基底

直交する偏光の組み合わせを基底と呼ぶ。

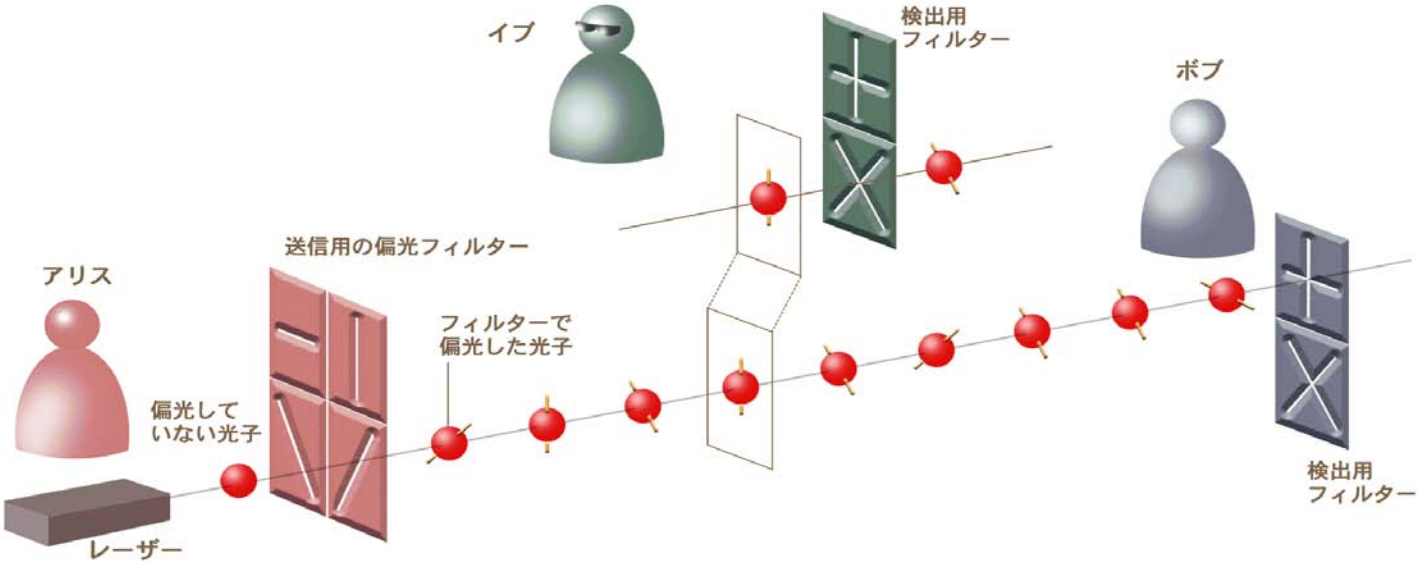
ベネットとブラッザードの量子暗号

ベネット

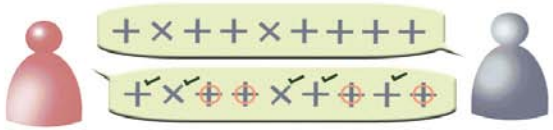


ブラッザード

プロトコル（操作手順）の概要



アリスが送った情報	0	0	1	0	1	0	1	1	1
アリスの送信用フィルター	／	|	＼	|	＼	／	＼	＼	—
ボブの検出用フィルター	+	+	+	+	×	+	+	×	+
ボブの検出結果	1	0	1	0	1	0	0	1	1
得られた暗号鍵	–	0	–	0	1	–	–	1	1

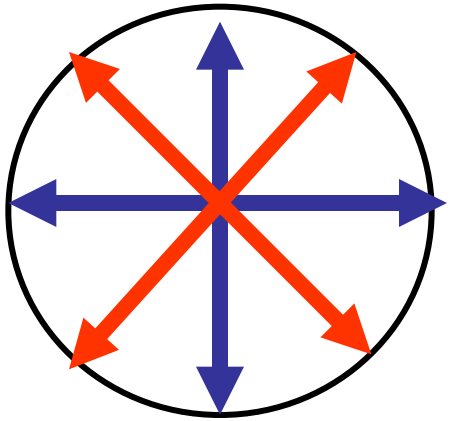


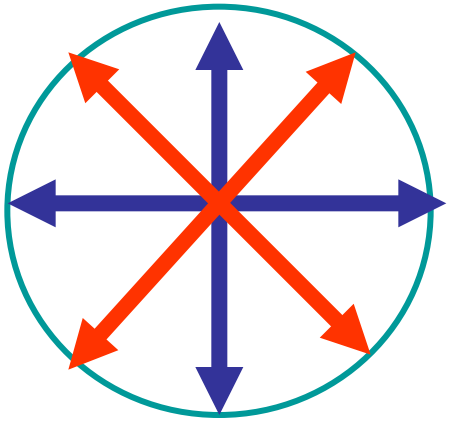
情報通信ベンチャー支援センター　現代暗号の動向とビジネス
http://www.venture.nict.go.jp/series/cryptography/chapter4/4_3.html より借用

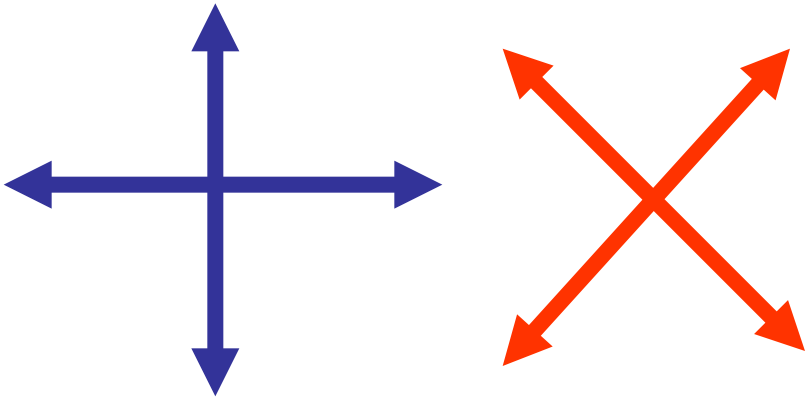
量子暗号 プロトコル

Alice

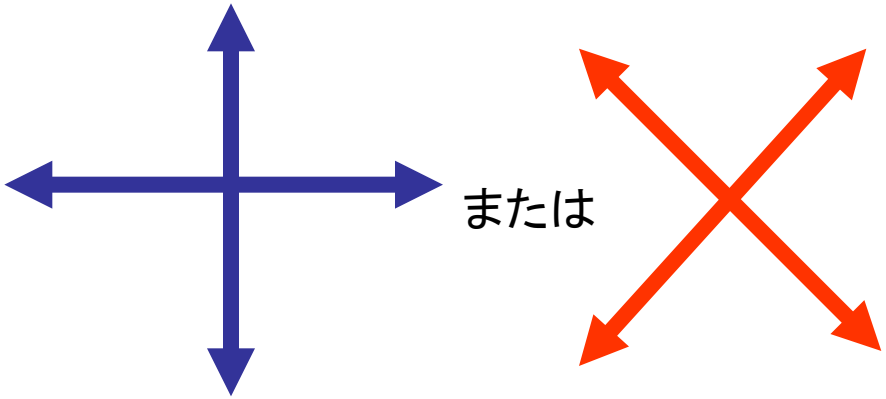
Bob







のどれか1つの状態を送る。



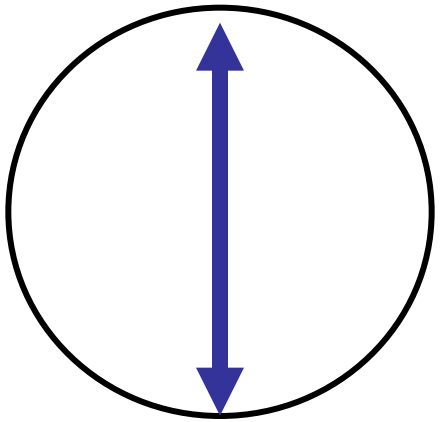
のどちらかの測定を行う。

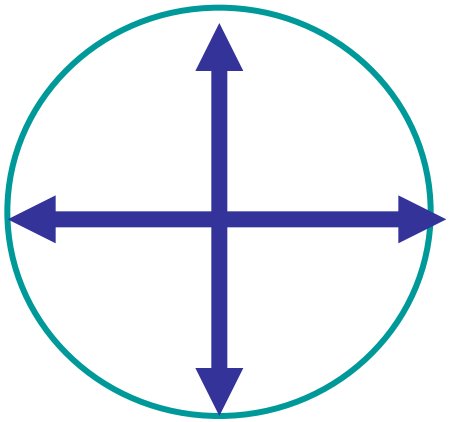
Alice と Bob が同じ基底を用いた場合

Alice

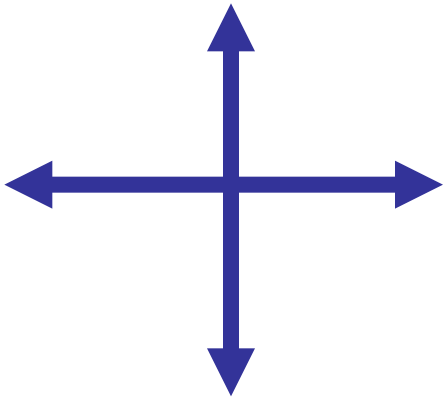
Bob

確率1





を送る

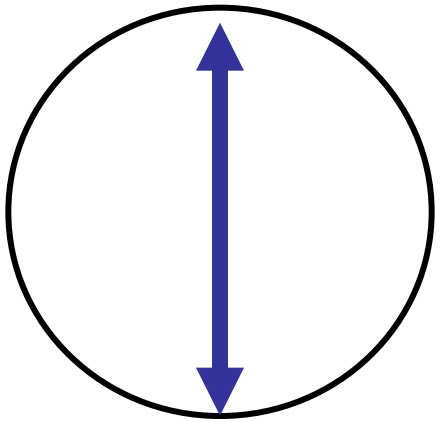


で測定する

Alice と Bob は同じ乱数（ビット）を共有できる

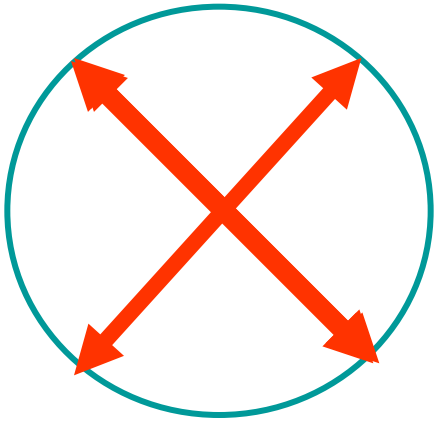
Alice と Bob が異なる基底を用いた場合

Alice

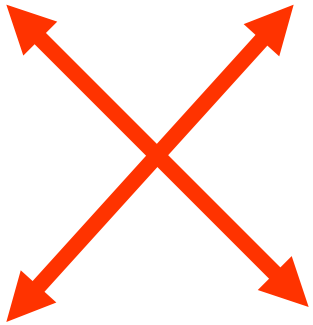


を送る

Bob



確率1/2

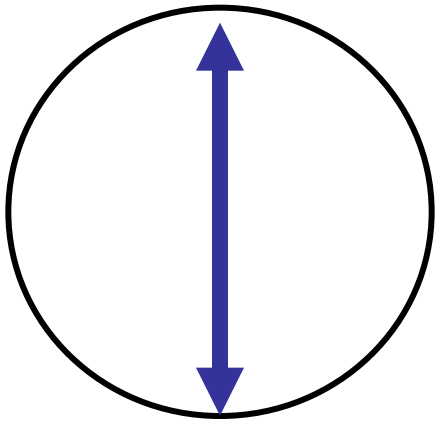


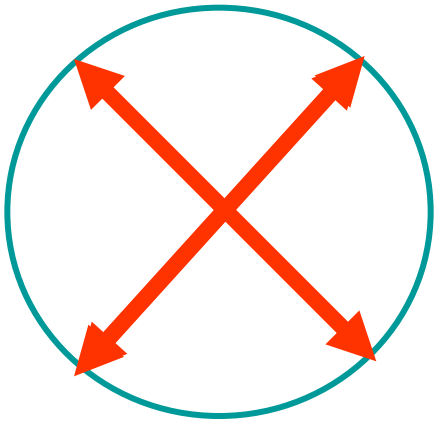
で測定を行う

Alice と Bob が異なる基底を用いた場合

Alice

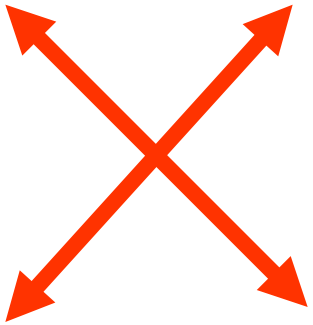
Bob





確率1/2

を送る

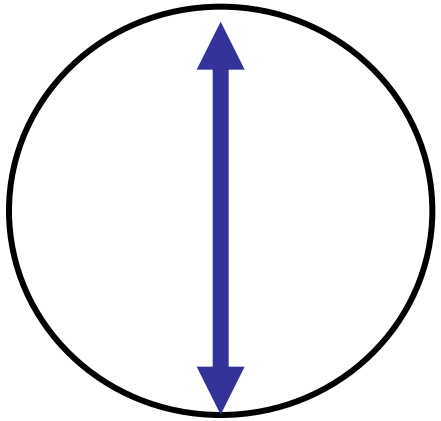


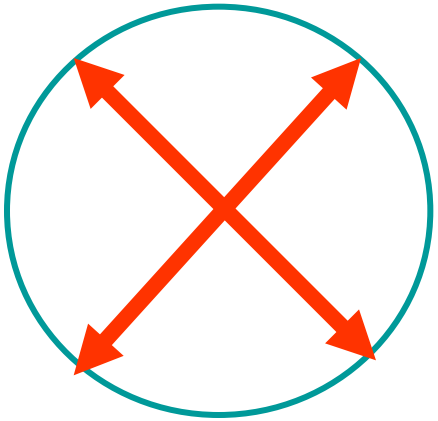
で測定する

量子通信終了後の手続き

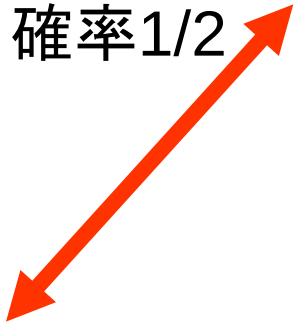
Alice

Bob



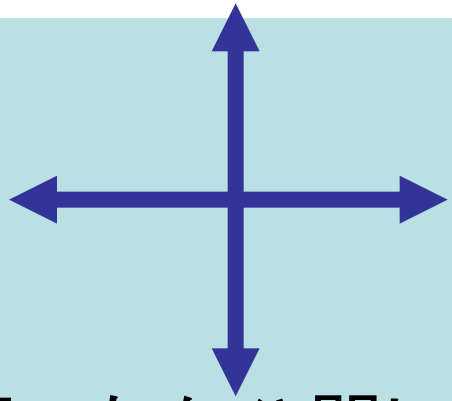


確率1/2

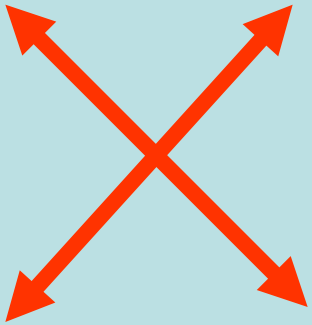


通信終了後,

Alice と Bob は



または



のどちらの基底を用いたか公開し、
両者の基底が一致した部分のビット情報のみ残す。
Alice と Bob は完全に一致したビットを共有できるはず！

Alice

Bob

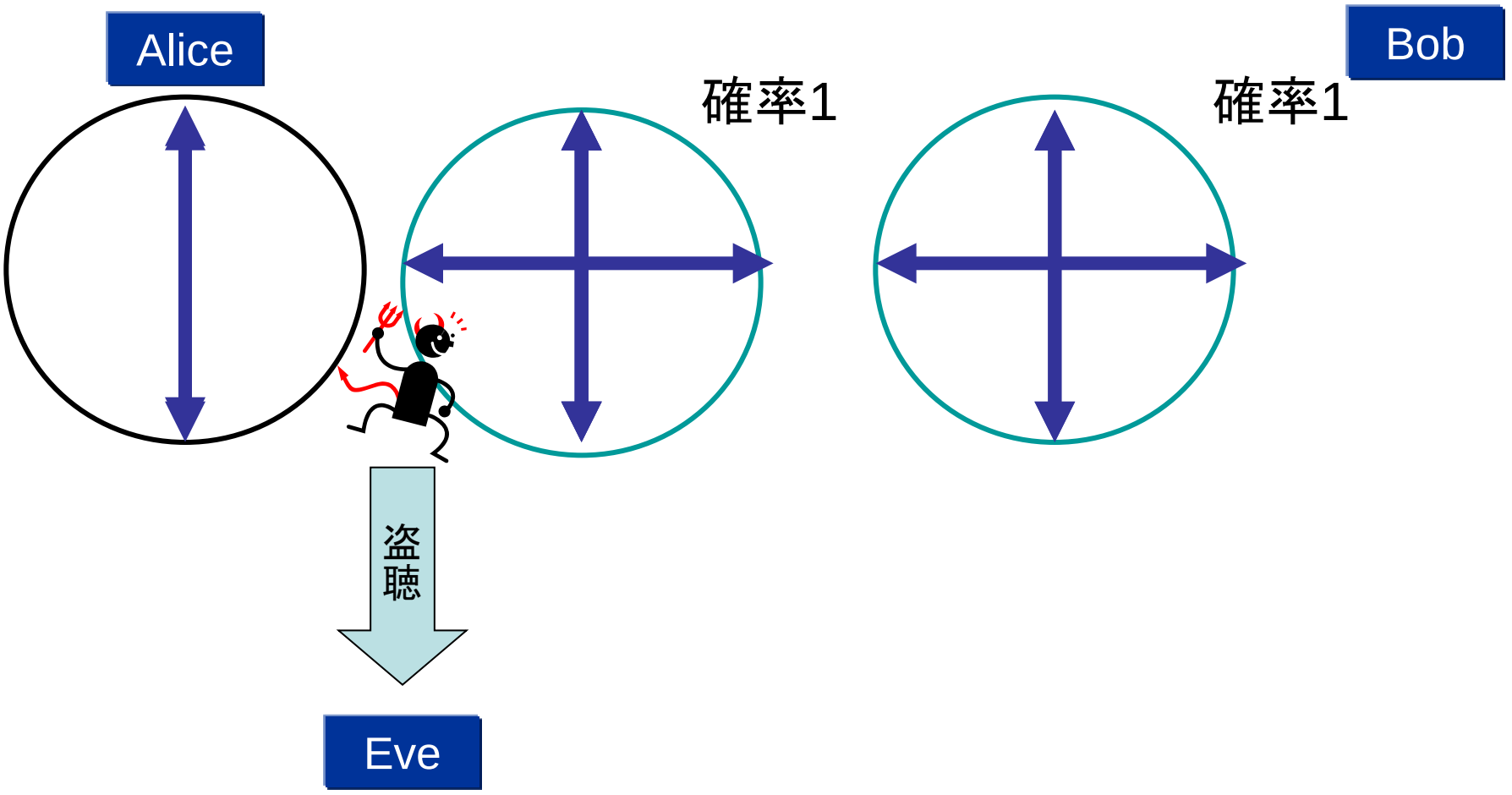
基底だけを送り，基底が一致した部分の情報だけを使う

ビット	基底	基底	ビット
0	＋	＋	0
0	＋	×	1
1	×	×	1
0	×	＋	0
0	＋	＋	0
1	×	×	1
0	×	＋	1
1	×	×	1
1	×	＋	1
0	＋	＋	0

本当に安全かな？

盗聴があった場合

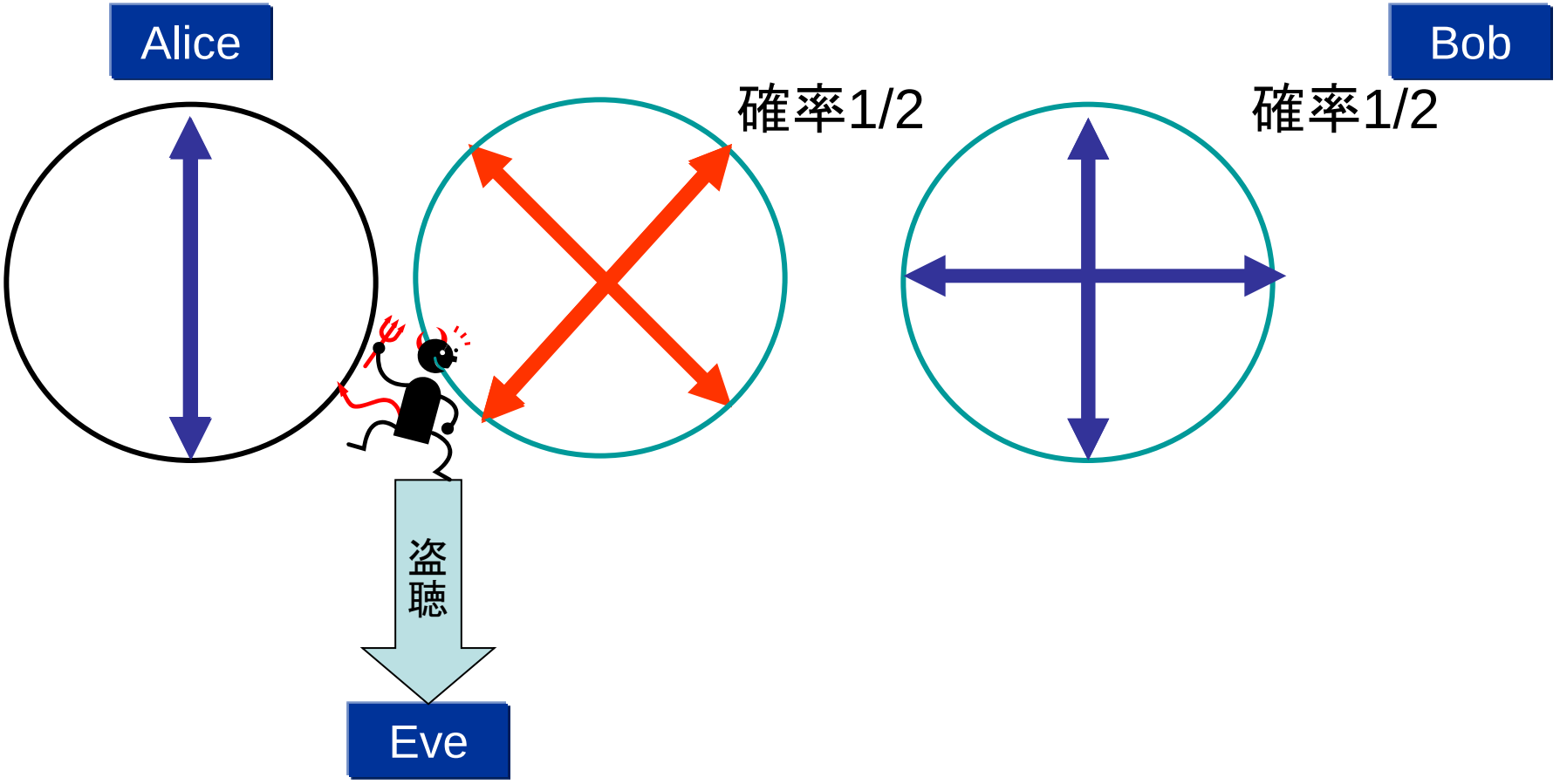
盗聴者 Eve が正しい基底で測定したとする。（確率1/2）



確率1で Eveは正しい情報を盗むことができる。
確率1でAliceとBobの鍵は一致する。

盗聴があった場合

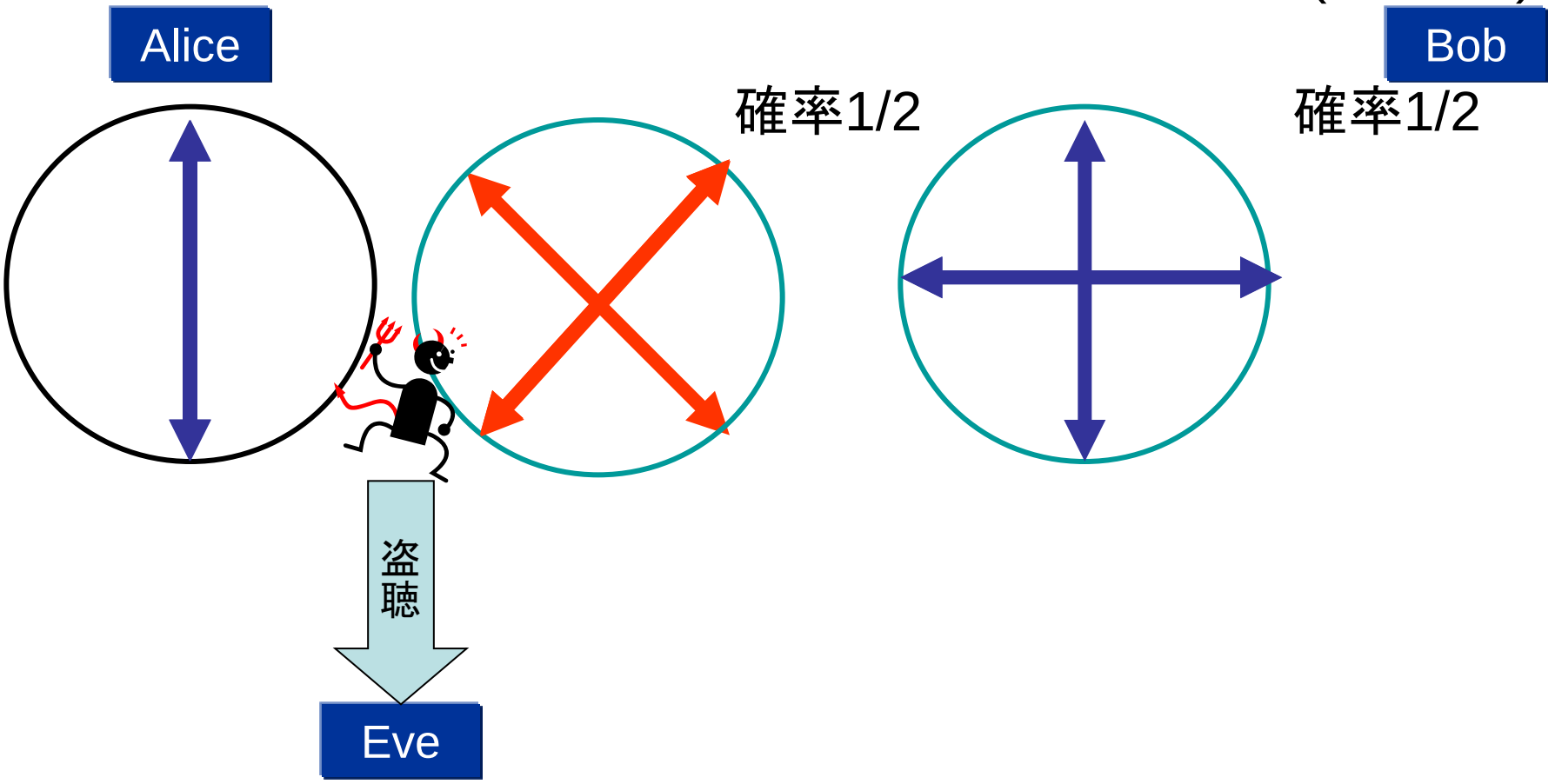
盗聴者 Eve が誤った基底で測定したとする。(確率1/2)



確率1/2でAliceとBobの鍵は一致する。

盗聴があった場合

盗聴者 Eve が誤った基底で測定したとする。(確率1/2)



確率1/2でAliceとBobの鍵は一致しない。

たくさん盗聴すれば，盗聴の痕跡が残る！

- Alice と Bob は基底が一致したビットのみ，残す。
- Eveが盗聴したとすると，確率1/2で誤った基底で測定してしまう。
- Eveが盗聴したとすると，確率1/2 × 1/2=1/4でAlice と Bob のビットは異なる。
- だいたい4回に1回はAlice と Bob のビットは異なる。

⇒たくさん盗聴すると必ず不一致が残る！

盗聴検証

盗聴を検出のため、通信終了後に、Alice と Bob は
基底照合を行い、基底が合ったビットのうちから
半分のビット（チェックビット）をランダムに選んで照合する。

盗聴があると、4ビットのうち1ビットの割合で、
不一致を検出！

おさらい

- 秘密の同一の乱数が準備できれば秘密の通信が出来る。
- 量子暗号も使えば、秘密の同一の乱数が準備できる。
- 量子暗号では、4種類の偏光を送る。
- 量子暗号では、基底の照合が必要！
- 量子暗号では、盗聴があったら検知できる。

量子暗号の要諦

目的

Eve にどのビットがどの基底に対応するか
分からないようにする.

手段

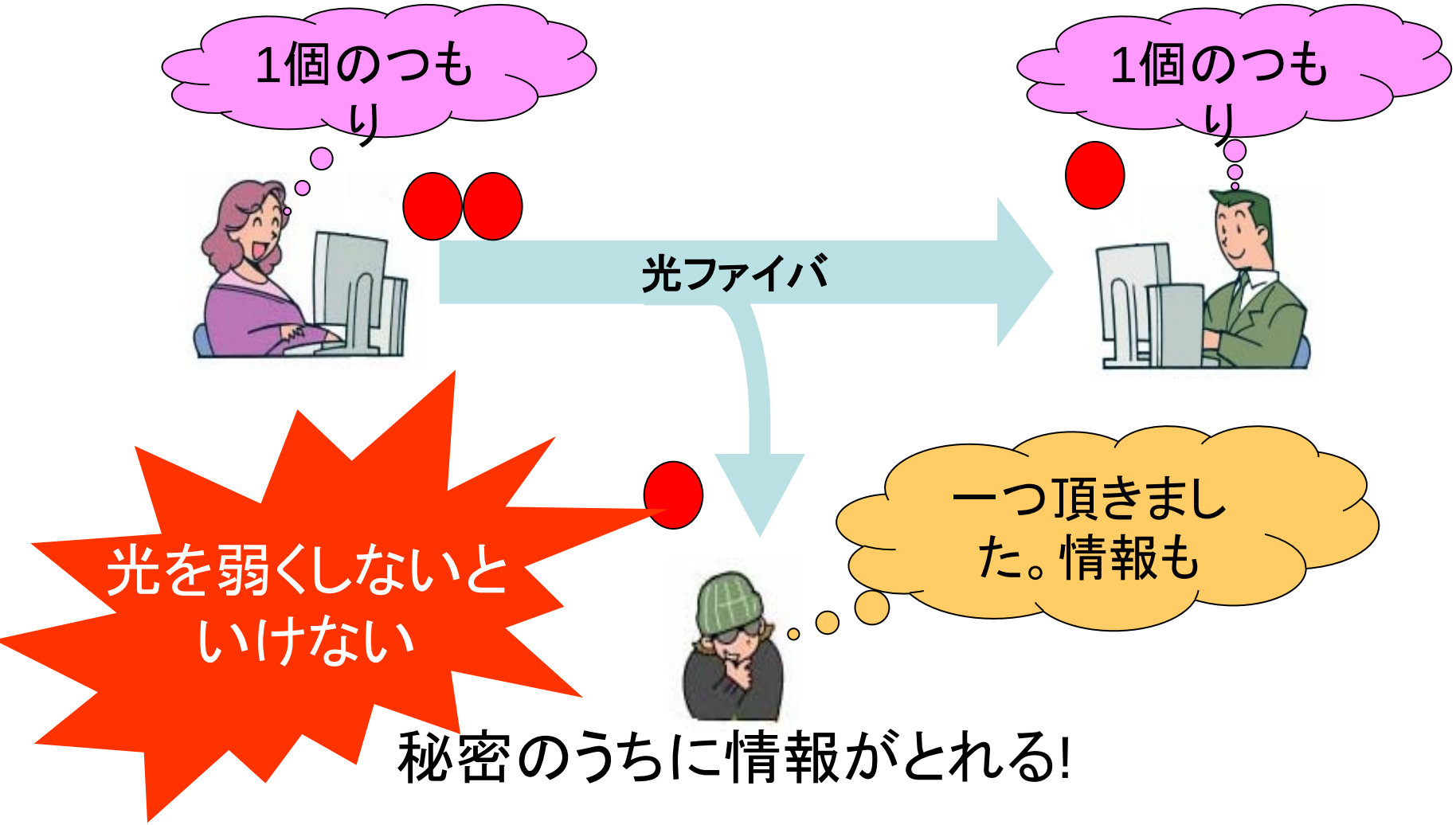
あらかじめ, Alice と Bob は
お互いに自分の基底を知らせずに通信を行う.

敵を騙すには，まずは味方から

偏光板と懐中電灯で量子暗号はできないの？

- 懐中電灯を用いた実験では、たくさんの光子が同時に出る。
- 光子が同時に2個出ると？

光子が同時に2個出ると？



秘密のうちに情報がとれる!

本当にベネット・ブラッザードの方法で大丈夫なの？

- ノイズがある
  ⇒ノイズにまぎれた盗聴の可能性
- 誤って2つ以上の光子を送ってしまう
  ⇒盗聴者が1光子を抜き取る盗聴の可能性

ノイズや不完全な光源の性質を利用して、盗聴者は部分的に情報を盗むことが出来る！

対策

生成した鍵から、
漏れた情報を取り除く必要がある！

秘匿性増強
―洩れた情報を取り除く技術―

肉を切らせて骨を絶つ！

どうやって
洩れた情報を取り除くの？
（秘匿性増強１）

3ビットの通信を行い、そのうち1ビットの情報が漏れたとする。
また、どのビットが漏れたか分からない。

$$\begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} \mapsto \begin{pmatrix} X_1 + X_2 \\ X_1 + X_3 \end{pmatrix}$$

ただし、
排他的論理和(XOR)
（1+1=0）

例え、盗聴者が X_1, X_2, X_3 のうちのどの1ビットの
情報を持っていても、最終的な情報は全く分からない。

しかし、鍵の長さが2/3 に減る。
対応できる盗聴者の情報量は1/3まで。

秘匿性増強2

6ビットの通信では、以下の方法では全ての2ビットの
情報漏えいに対応できない。

$$\begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \\ X_6 \end{pmatrix} \mapsto \begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \end{pmatrix} = \begin{pmatrix} X_1 + X_2 \\ X_1 + X_3 \\ X_4 + X_5 \\ X_4 + X_6 \end{pmatrix}$$

先の秘匿性増強プロトコルを2回繰り返したもの

X_1, X_2 が分かってしまうと、 Y_1 が分かってしまう。

秘匿性増強３

7ビットの通信を行い、そのうち2ビットの情報が漏れたとする。
また、どのビットが漏れたか分からない。

$$\begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \\ X_6 \\ X_7 \end{pmatrix} \mapsto \begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \end{pmatrix} = \begin{pmatrix} X_1 + X_4 + X_5 + X_7 \\ X_2 + X_4 + X_6 + X_7 \\ X_3 + X_5 + X_6 + X_7 \\ X_1 + X_2 + X_3 + X_4 + X_5 + X_6 + X_7 \end{pmatrix}$$

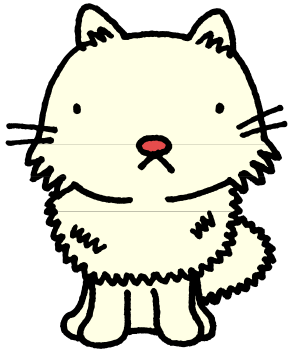
鍵の長さが4/7に減る 。対応できる盗聴者の情報量は2/7まで。

実際はもっと大きなサイズで処理を行う。

本当に大丈夫かな？

- 確認するには、盗聴者がどの2ビットを知っているときでも、変換後のビットが(0,0,0,0)になる確率が,同じであることを確認すればよい。
- たとえば、X_1, X_2を知っているとき、変換後のビットが(0,0,0,0)になる入力ビットの組み合わせは8個である。このうち、X_1, X_2 が、(0,0),(1,0),(0,1),(1,1)になる組み合わせが全て同じ個数（2個）であることを確認するとOK！

確認してみる!?

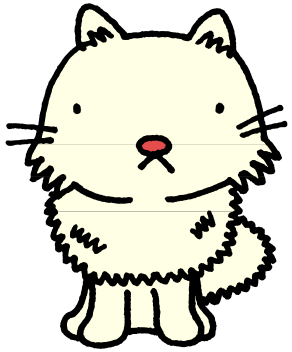


$(Y_1, Y_2, Y_3, Y_4) = (0,0,0,0)$ となる場合の内訳

(X_1, X_2)	$(X_1, X_2, X_3, X_4, X_5, X_6, X_7)$	
$(0,0)$	$(0,0,0,0,0,0,0)$	$\frac{2}{2^5} = \frac{1}{2^4} = \frac{1}{16}$
	$(0,0,1,0,1,1,1)$	
$(1,0)$	$(1,0,1,1,0,1,0)$	$\frac{2}{2^5} = \frac{1}{2^4} = \frac{1}{16}$
	$(1,0,0,1,1,0,1)$	
$(0,1)$	$(0,1,0,1,0,1,1)$	$\frac{2}{2^5} = \frac{1}{2^4} = \frac{1}{16}$
	$(0,1,1,1,1,0,0)$	
$(1,1)$	$(1,1,0,0,1,1,0)$	$\frac{2}{2^5} = \frac{1}{2^4} = \frac{1}{16}$
	$(1,1,1,0,0,0,1)$	

(X_1, X_2) だけが漏れた場合は大丈夫！

より一般には。。。



$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

上の行列の中から任意の2つの列ベクトルを取り除いた場合に、
行列のランクが4であることを確認するとよい。

秘匿性増強４

以下の秘匿性増強行列を用いて、10ビットを4ビットに変換する。
このとき、ほとんどの5ビットの組み合わせが盗聴されていても安全！

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

上の行列の中からほとんどの５つの列ベクトル組み合わせのついて
これらからなる行列のランクが４である。

秘匿性増強4

ランクが4とならない例

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

そのような組み合わせ $\binom{4}{2} \times 2 + \binom{4}{3} \times 3 = 24$

ランダムに選んだ場合そのようになる確率

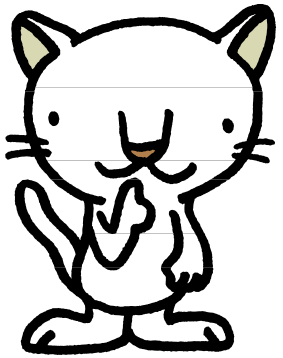
$$24 \Big/ \binom{10}{5} = \frac{1}{21}$$

非常に小さい

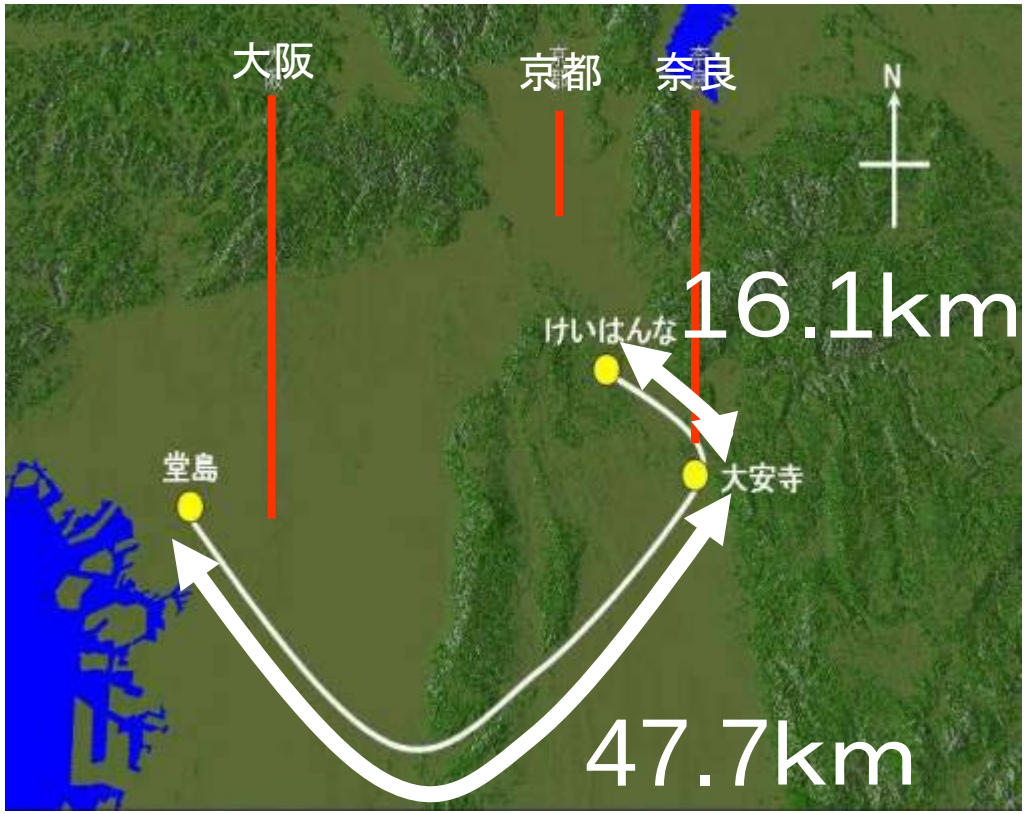
サイズを大きくするとこの確率は0に近づく

どうやって量子暗号を実現するの？

- 普通の光通信で使っている光ファイバーを使う方法
- 空気中に光子を飛ばす方法
- 人工衛星を用いる方法
- どの方法でも、通信に使う光を非常に弱くしないといけない。



都市圏敷設ファイバーでの量子暗号
世界最長距離



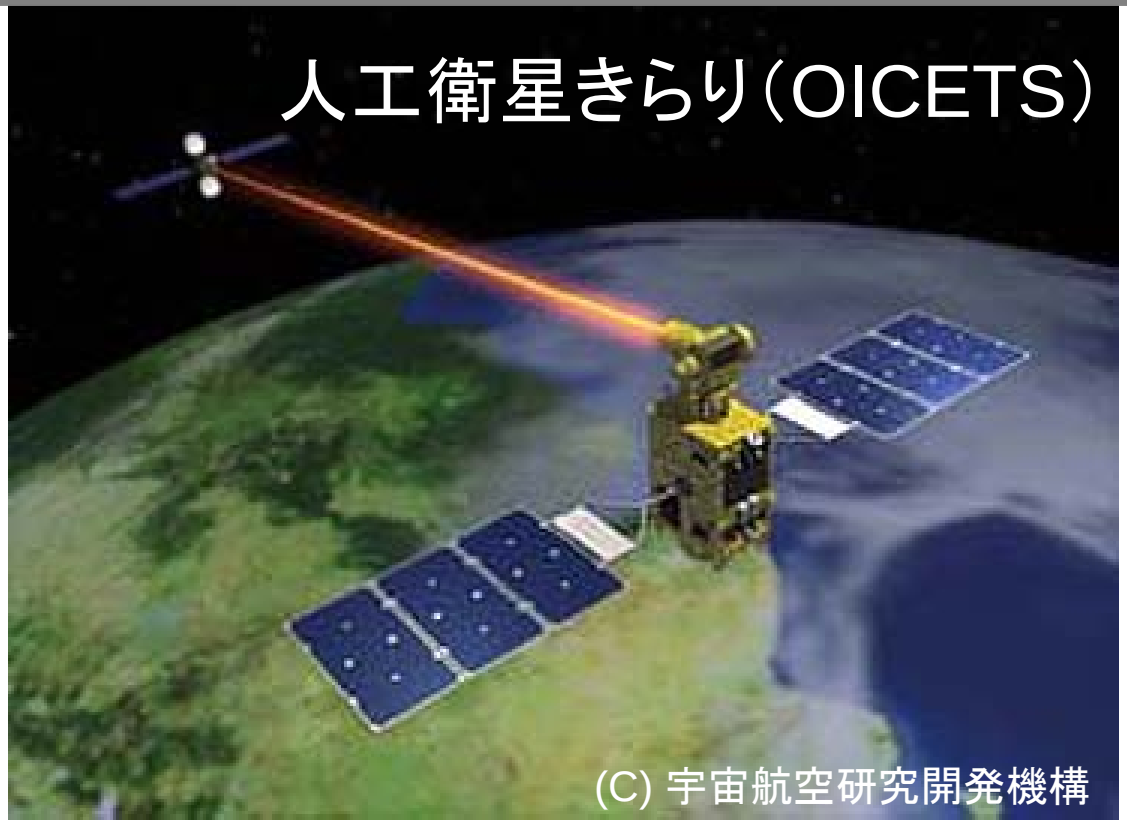
47.7km
+3×16.1km
=96km　三菱電機

3往復(16.1km)
+0.4km
=97km　NEC

三菱電機（2004），NEC（2008）（最高速）による実験
共に情報通信研究機構(NICT)による受託研究
スイス，アメリカでも同様の実験

清水克宏(三菱電機)「JGN2光テストベッドを用いた 量子暗号システム試験」
JGNIIシンポジウム2005in大阪．http://www.jgn.nict.go.jp/sympo2005/

深宇宙光通信



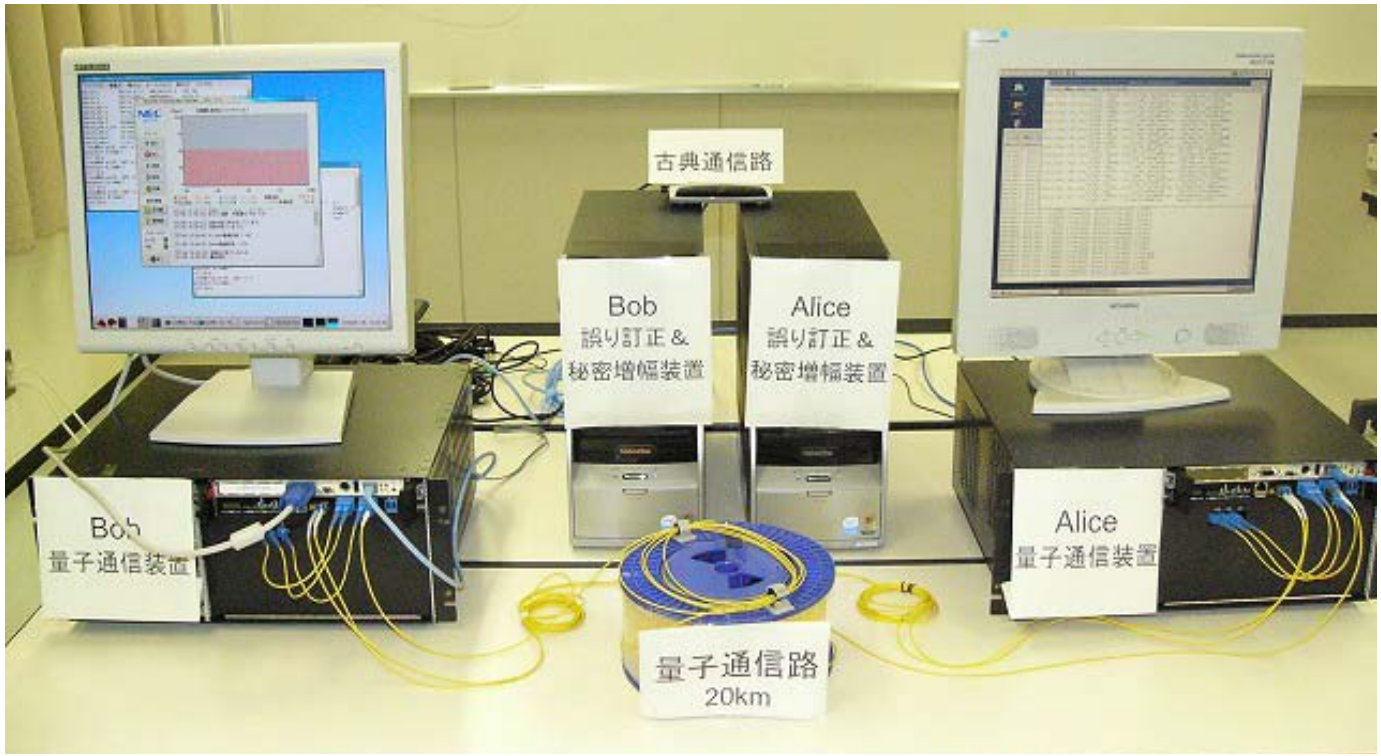
宇宙基本法
2008年
5月21日成立

情報通信機構（日本）きらり（OICETS）
ヨーロッパ宇宙局（ヨーロッパ）アルテミスが
人工衛星を用いた地球規模での量子暗号！
宇宙空間では障害となる大気が無いのが利点！

量子暗号発展の主な歴史

- 1984 ベネット，ブラッザードによるプロトコルの提案
- 1996 メイヤーズによるノイズがある場合のプロトコルの改良、及び安全性の証明
- 2003 ファンによるおとり法の提案（不完全な光源に対する対策）
- 2007 林により不完全な光源で定量的な安全性が示される
- 2007 林らにより、定量的に安全性を保証できる量子暗号装置の作成（従来のシステムでは安全性は保証されていなかった．）
  ⇒次の写真

安全性保証付き量子暗号装置



実験環境

光ファイバ 20km
通常のオフィス環境
（ERATO-SORST
東京オフィス）

量子通信装置

NEC製を改造
（送信強度：4種類）
波長 $1.55\mu m$
システムクロック 62.5 MHz
Plug and Play 方式

誤り訂正・秘匿性増強装置

PC （LINUX)
CPU:
Pentium(R)4(3GHz)
メモリ: 2GB

JST ERATO-SORTによる実装実験

量子暗号はいつごろ実用化されるの？

スイスが選挙のための利用を検討中！

Science & Technology

Quantum cryptography

Un

Heisenberg's certainty principle

Oct 18th 2007

From *The Economist* print edition

The Swiss are using quantum theory to make their election more secure

HANGING chads. Ballot stuffing. Gerrymandering. Such dirty tricks enfeeble democracy. But the security of the votes cast in Geneva during Switzerland's general election on October 21st is guaranteed. The authorities will use quantum cryptography—a way to transmit information that detects eavesdroppers and errors almost immediately—to ensure not only that votes are kept secret but also that they are all counted.