微(かす)かな光の不思議な世界

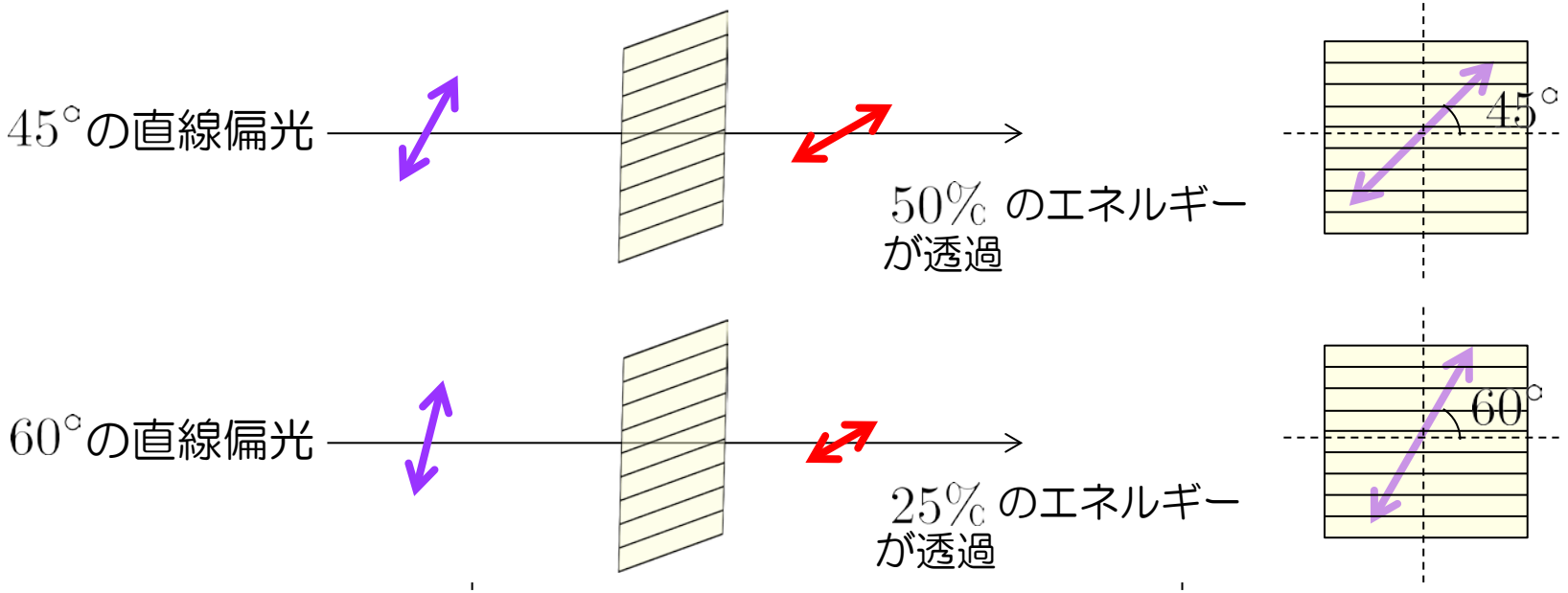
- 第11回　1/10　微弱光を用いた究極の暗号
  - 前回の復習と補足
  - 量子暗号のしくみ
  - もっと遠くへ～量子中継
  - 量子力学を超えて

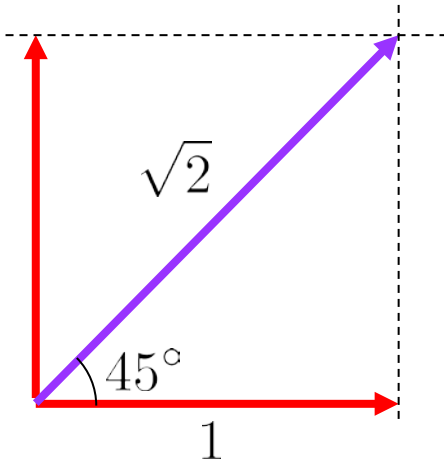
工学系研究科　光量子科学研究センター
物理工学専攻
小芦　雅斗

光の偏光と偏光フィルター

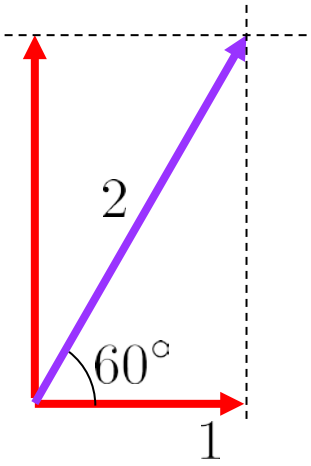
(横から見た図)

(光の進行方向から見た図)





入力：出力
$= (\sqrt{2})^2 : 1^2$
$= 2 : 1$

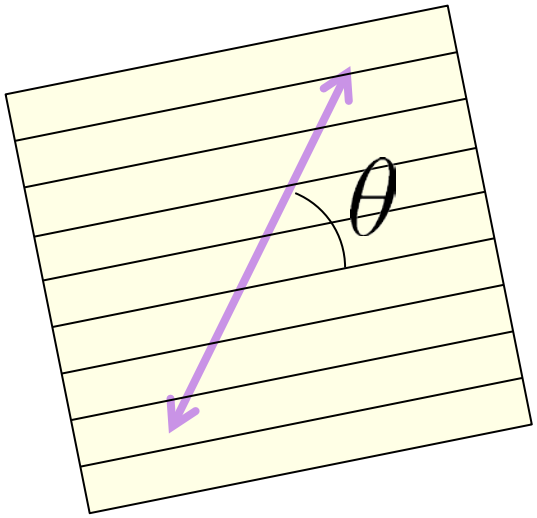


入力：出力
$= 2^2 : 1^2$
$= 4 : 1$

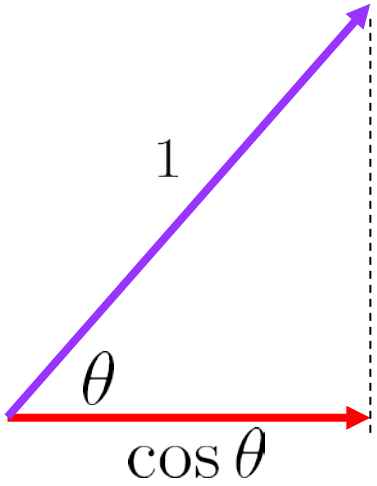
光の強さ、パワー、エネルギーなどは、振幅の２乗に比例

光の偏光と偏光フィルター

一般には・・・

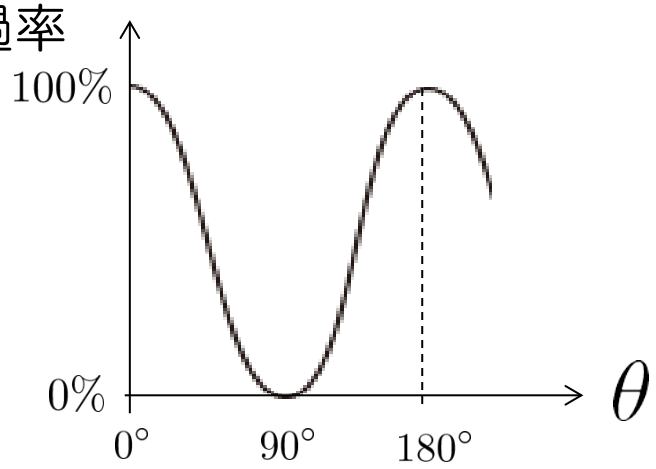


光の強さ、パワー、
エネルギーなどは、
振幅の２乗に比例



入力：出力
$= 1^2 : (\cos\theta)^2$

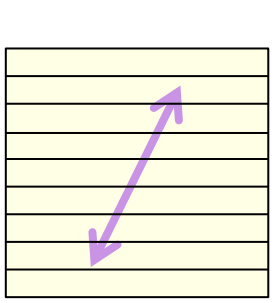
透過率



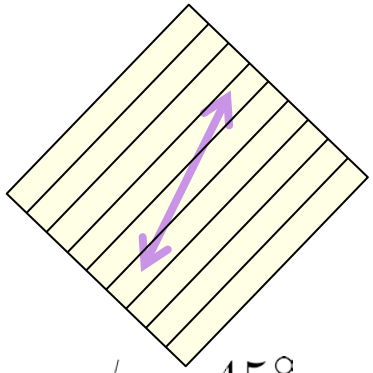
透過する割合は $(\cos\theta)^2$

光の偏光方向を測る

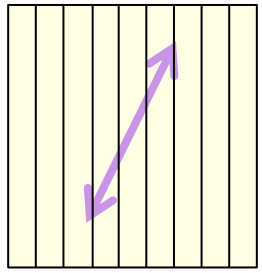
いろいろな角度にフィルターを置いて、透過率を調べる。



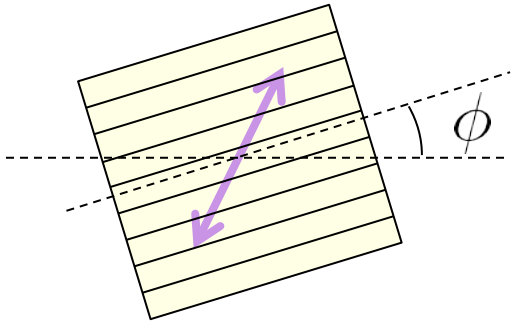
$\phi = 0°$

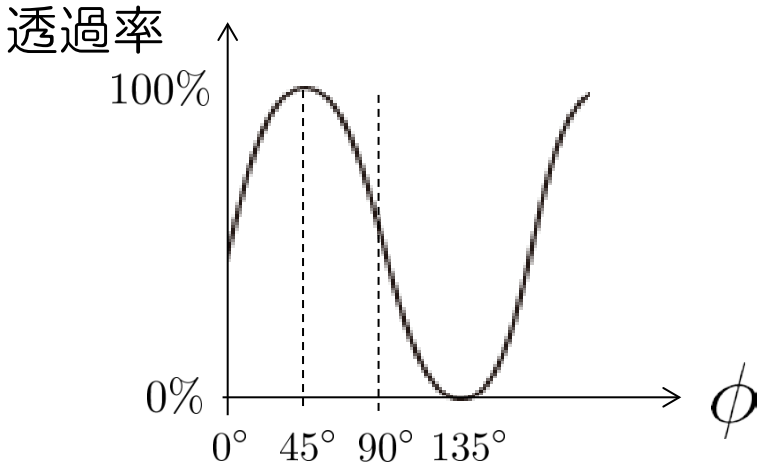


$\phi = 45°$



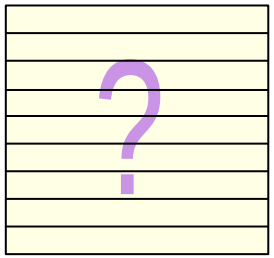
$\phi = 90°$



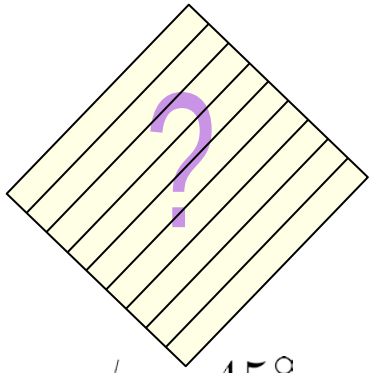


光の偏光方向を測る

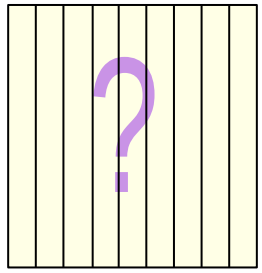
いろいろな角度にフィルターを置いて、透過率を調べる。



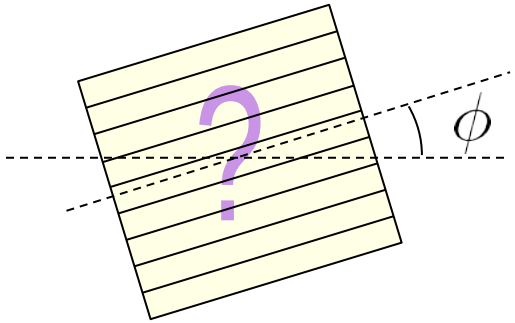
$\phi = 0°$

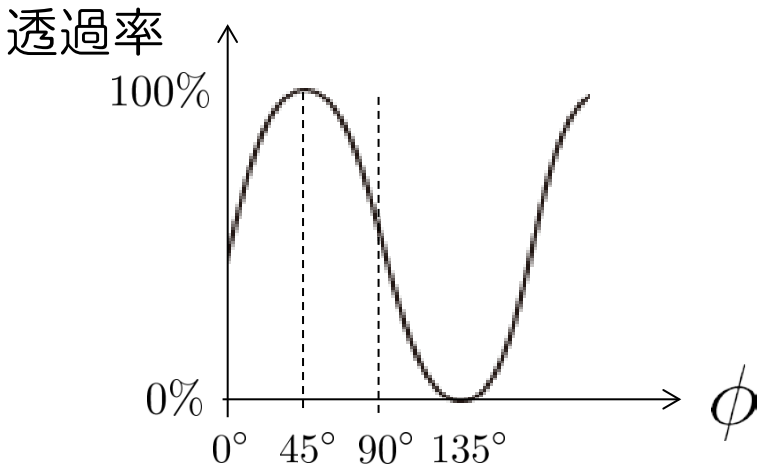


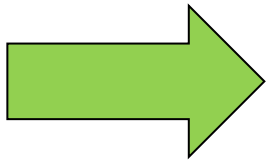
$\phi = 45°$

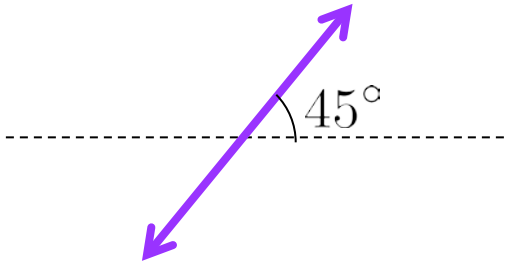


$\phi = 90°$



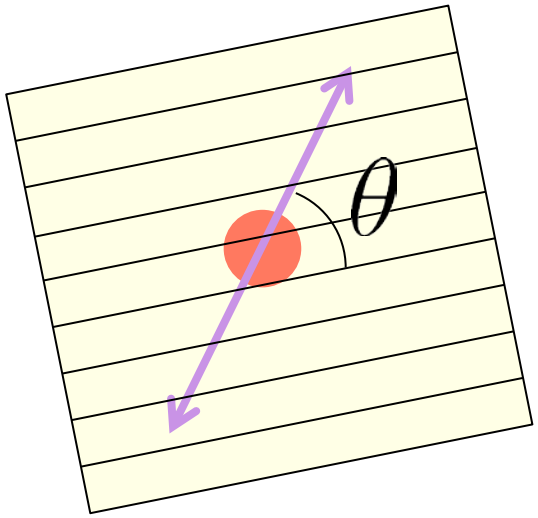


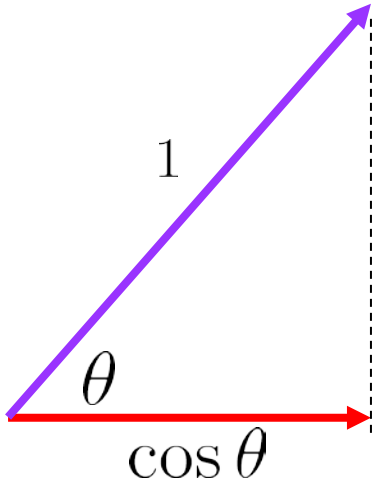




光子の偏光と偏光フィルター

光子の場合は・・・

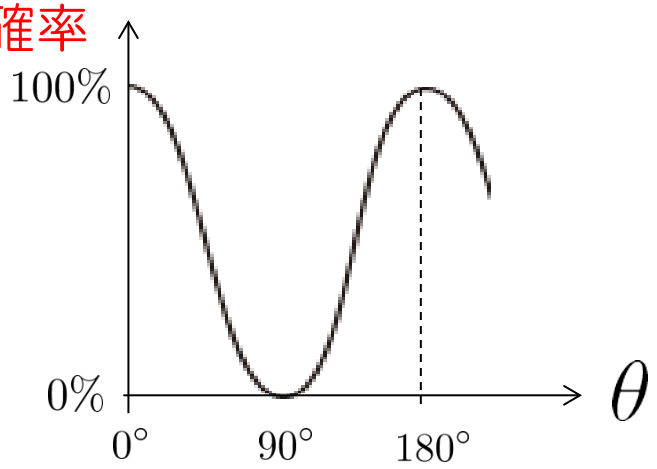




光子が透過する確率は

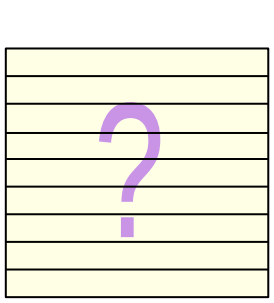
$$(\cos\theta)^2$$

透過確率

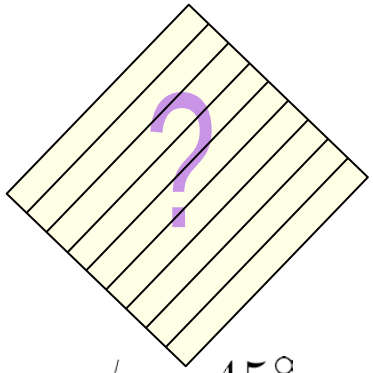


光子の偏光方向を測る

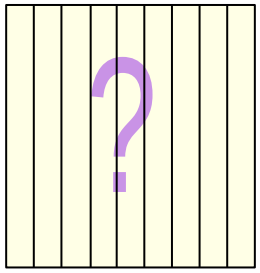
いろいろな角度にフィルターを置いて、透過確率を調べる。



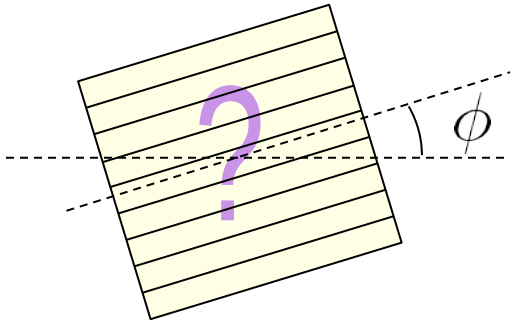
$\phi = 0°$



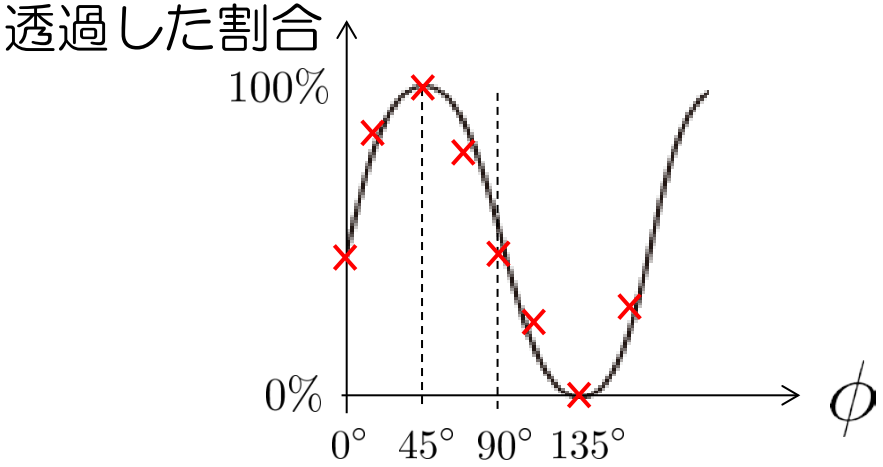
$\phi = 45°$



$\phi = 90°$



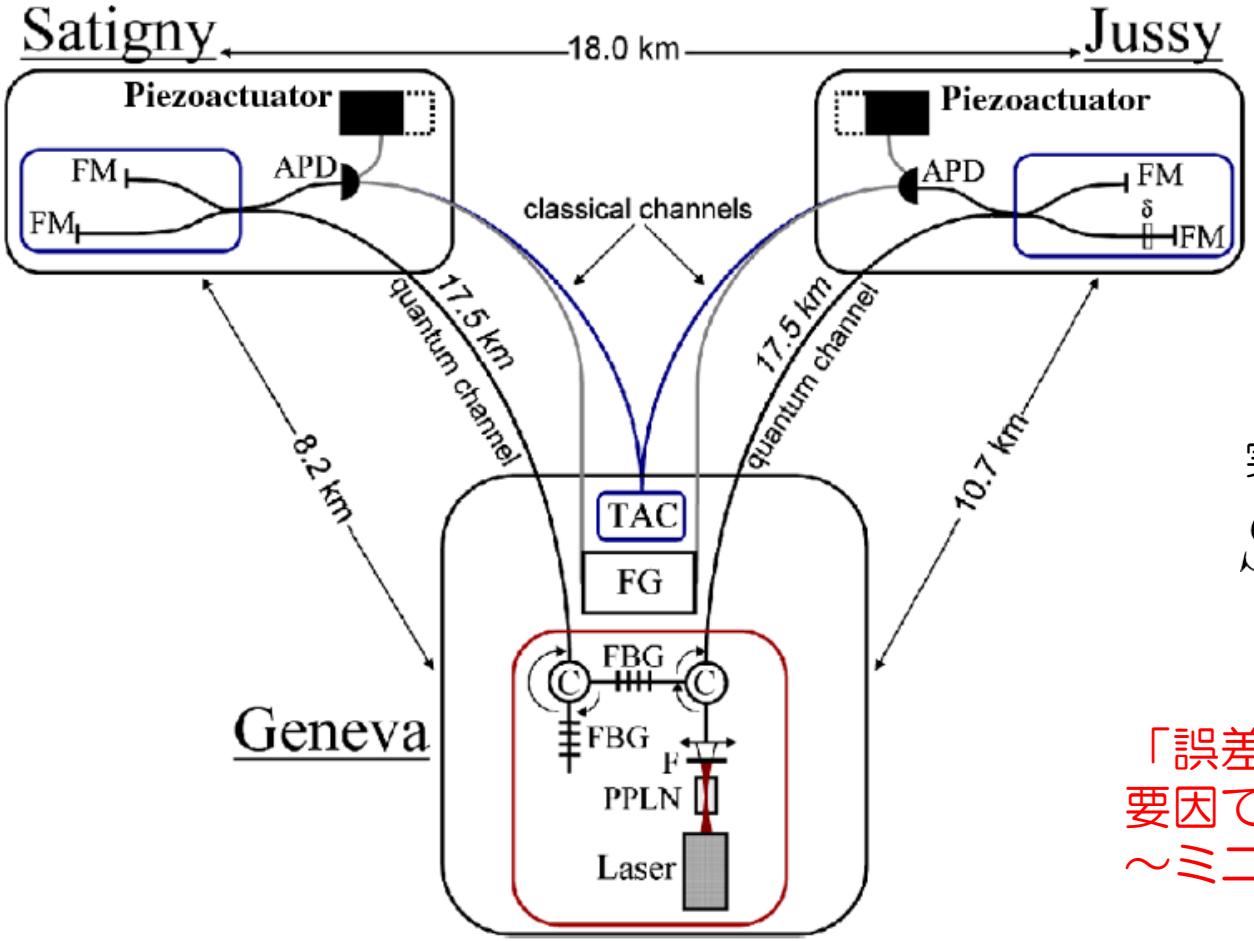
同じ偏光の光子をたくさん用意して、透過した個数の割合を測定



確率現象なので、誤差が生じる

N 個測ると相対誤差が
だいたい $1/\sqrt{N}$ 程度

CHSH不等式の破れの実験例



18km: 光速で　60 μ秒

測定は　７μ秒で完了

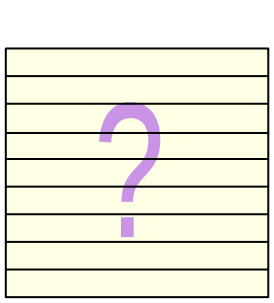
実験結果

$$S = 2.56 \pm 0.04$$

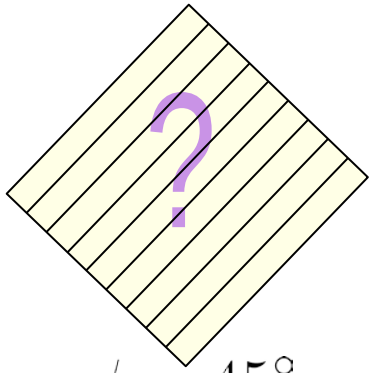
「誤差±０．０４はどのような要因で生じているのか？」
～ミニッツレポートより

光子の偏光方向を測る

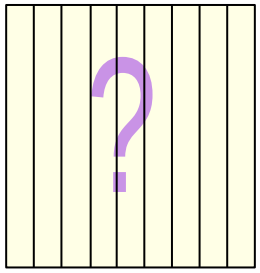
いろいろな角度にフィルターを置いて、透過確率を調べる。



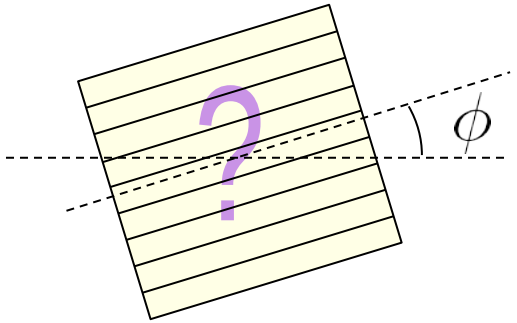
$\phi = 0°$



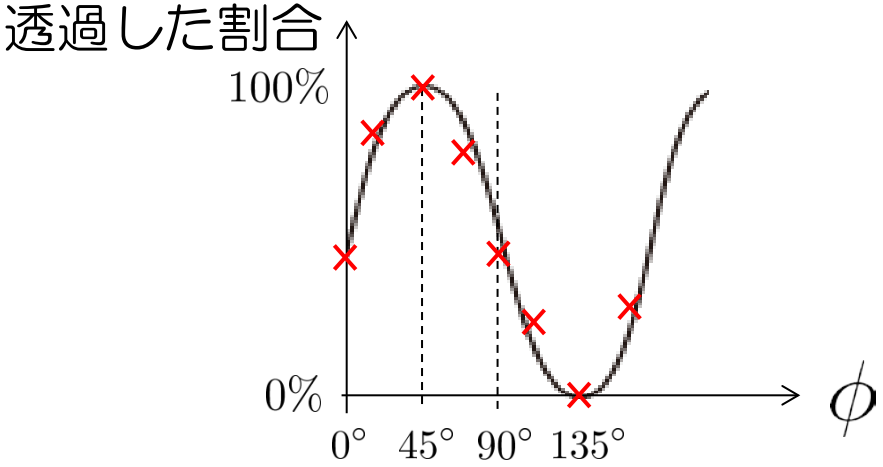
$\phi = 45°$



$\phi = 90°$



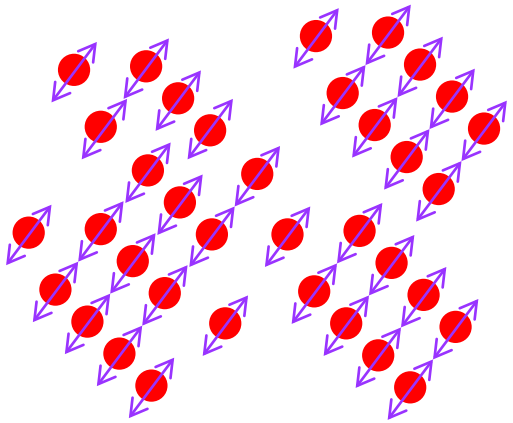
同じ偏光の光子をたくさん用意して、透過した個数の割合を測定



確率現象なので、誤差が生じる

N 個測ると相対誤差が
だいたい $1/\sqrt{N}$ 程度

光子の偏光方向を測る



測定によって偏光方向を
悪くない精度で決定できる。

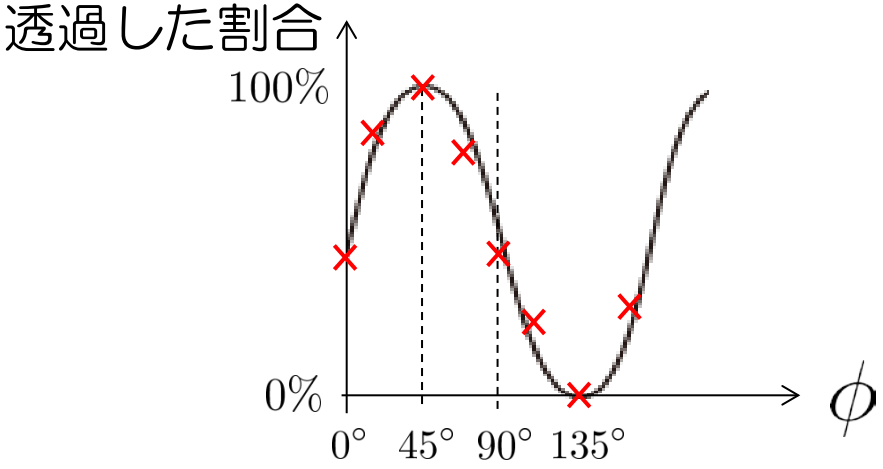
ϕ

$\phi = 0$ 45 $\phi = 90$

同じ偏光の光子をたくさん用意して、透過した個数の割合を測定

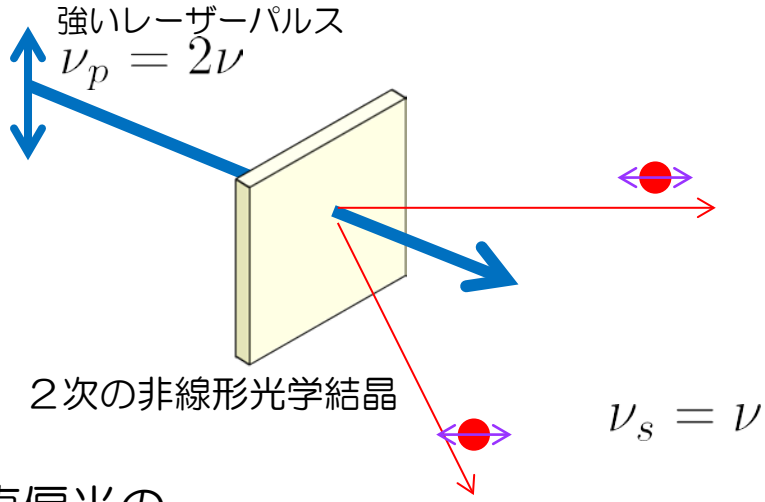
確率現象なので、誤差が生じる

N 個測ると相対誤差が
だいたい $1/\sqrt{N}$ 程度



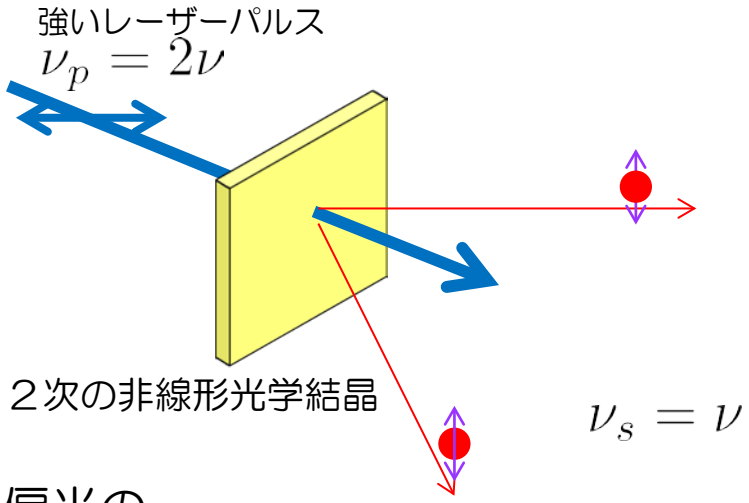
双子の光子対

光パラメトリック過程



垂直偏光の
$h\nu_p$ の光子１個が、

水平偏光の
$h\nu_s$ の光子２個に変換される

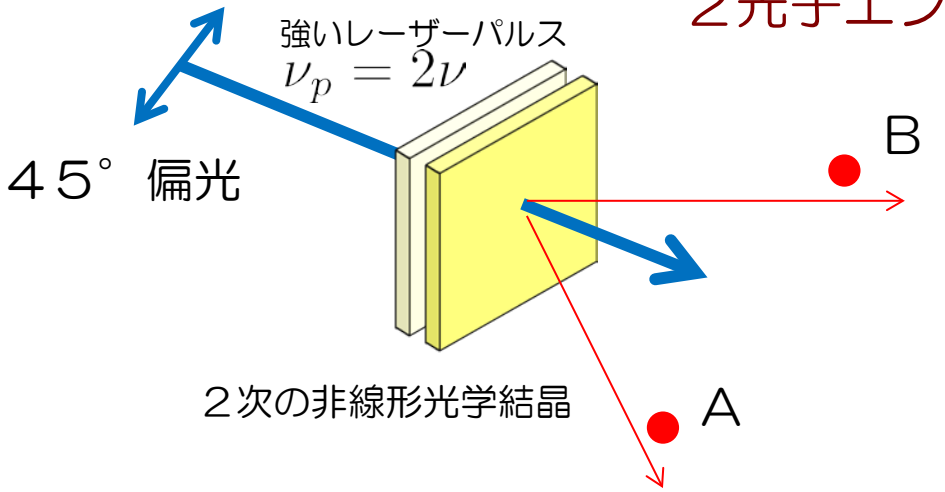


水平偏光の
$h\nu_p$ の光子１個が、

垂直偏光の
$h\nu_s$ の光子２個に変換される

双子の光子対

２光子エンタングル状態



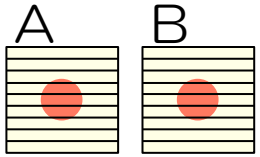
２枚がさねの板を用いて、

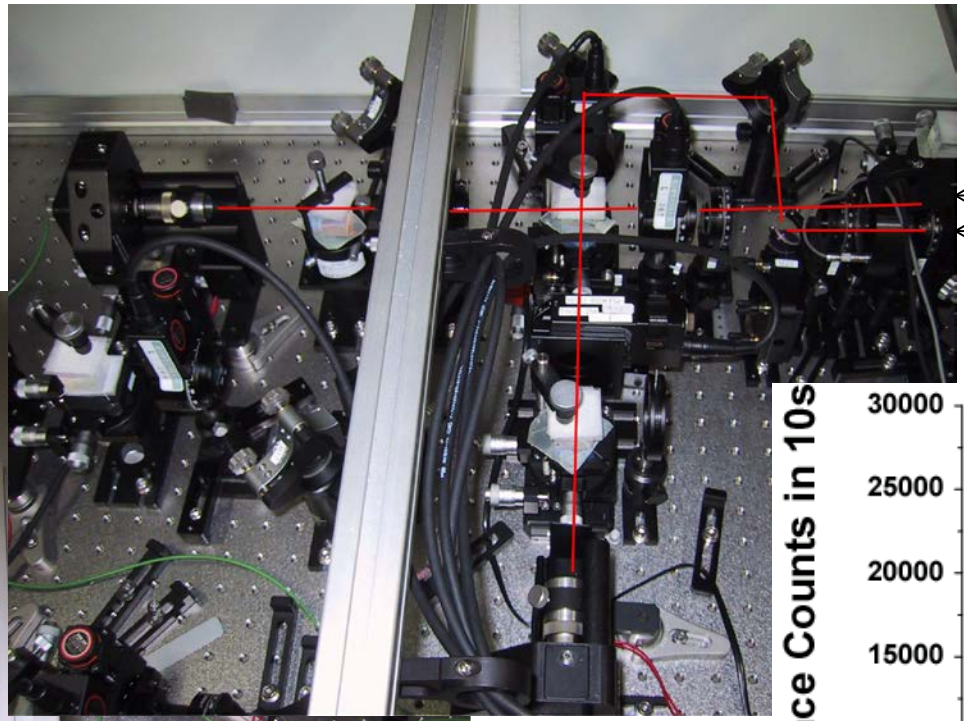
斜め４５°偏光の $h\nu_p$ の光子１個を、$h\nu_s$ の光子２個に変換する。

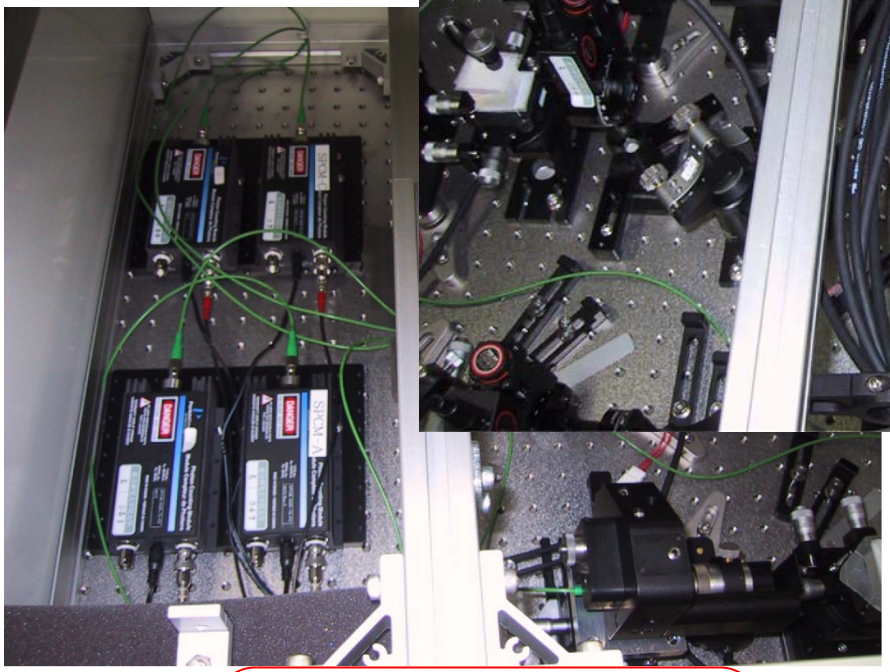
（２光子エンタングル状態）

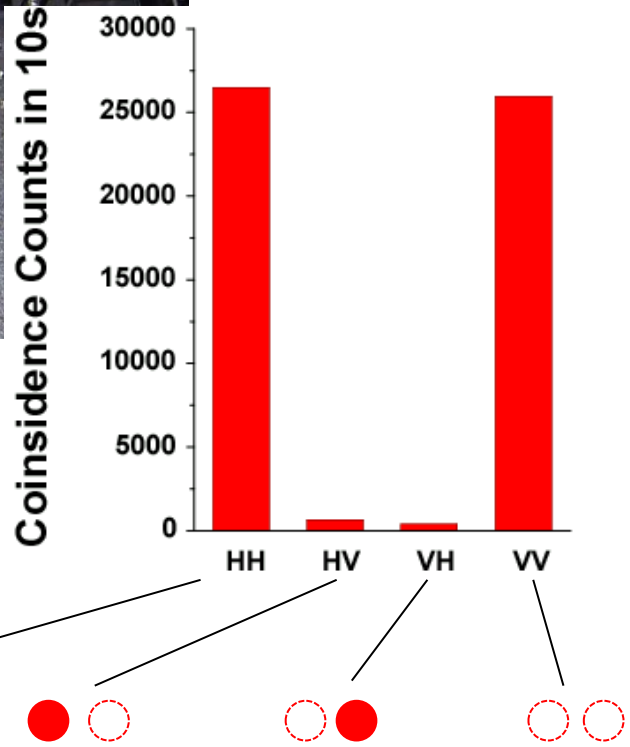
２種類の生成過程が重なると....

光子対と偏光フィルター





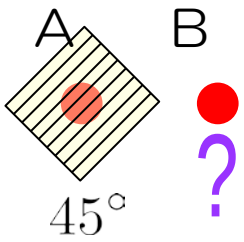


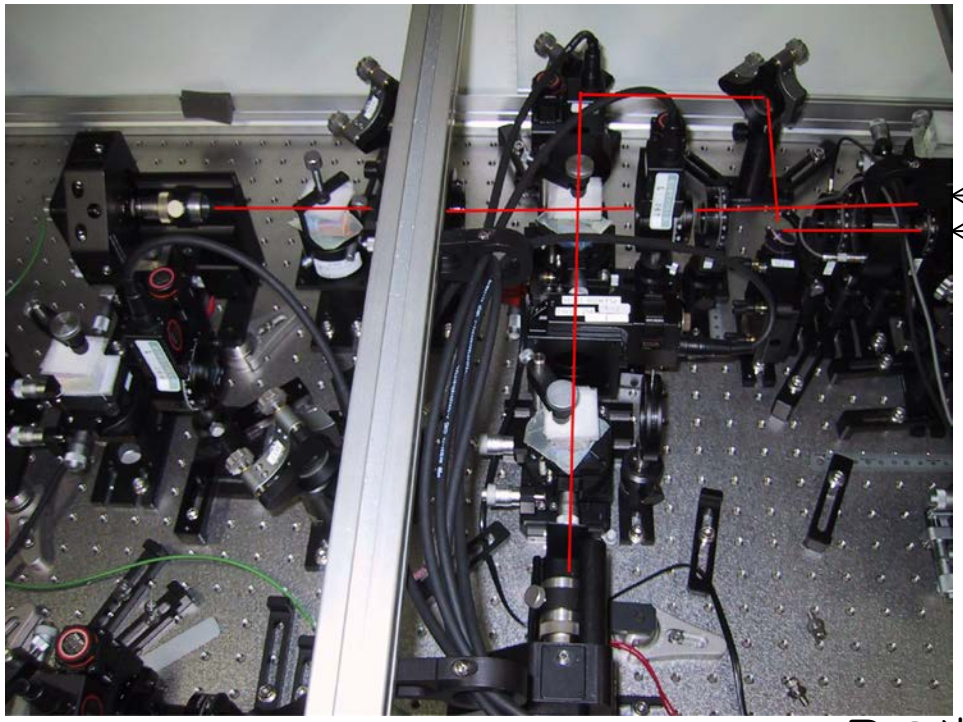


● 通り抜ける
（検出される）

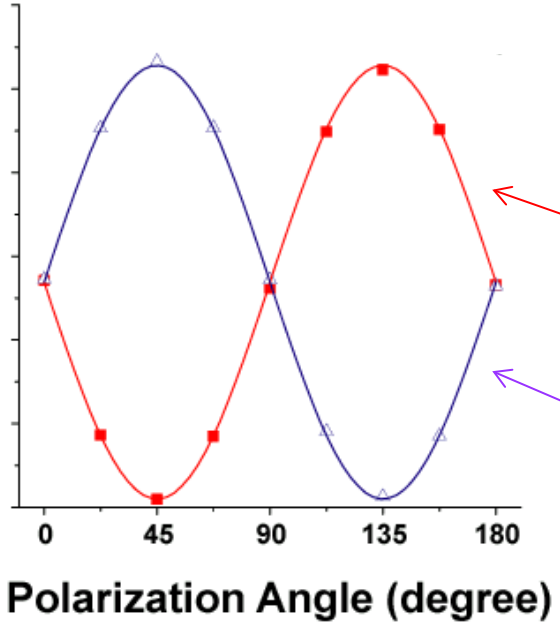
○ 通り抜けない
（検出されない）

光子対と偏光フィルター



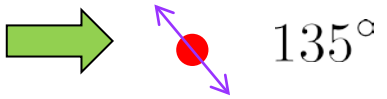


Bの光子が
透過した割合

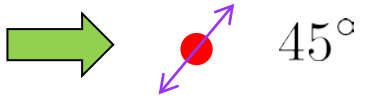


Bの光子

Aの光子がフィルターを
通り抜けない場合



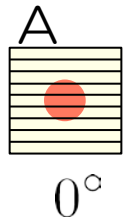
Aの光子がフィルターを
通り抜けた場合

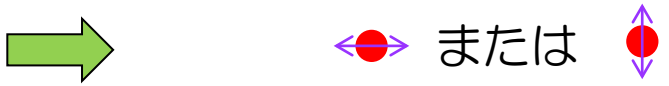


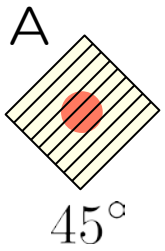
光子対と偏光フィルター

Aの光子に置いたフィルター

実験結果の示す
Bの光子の偏光







Aの光子に起きたことを、Bの光子が感知して偏光がかわったように見える。

何か未知の信号がAからBに伝わったと考えたくなるが、
AとBの光子を遠く離して、フィルターの向きの切り替えとB光子の測定をどんなに素早く行っても同じ現象が見られる。
つまり、そのような信号があるなら、光速より速く伝わらなければならない。

特殊相対性理論と光速

著作権の都合により、
ここに挿入されていた画像を
削除しました。

「ニュートリノ光より速い
相対性理論と矛盾」

読売新聞
2011年9月24日朝刊1面

２０１１年の記事

光速より速く何かが伝わるような話が出てくると、大騒ぎになるのはなぜだろう？

２０１２年の記事

著作権の都合により、
ここに挿入されていた画像を削除しました。

「ニュートリノ光速超えず
名古屋大など国際チーム　実験結果撤回へ」

日本経済新聞
2012年6月3日朝刊28面

絶対的に静止しているのは？

天動説：地球が世界の中心で、動かない。

地動説：地球は太陽の周りをまわっている。

ならば、動かないのは太陽？

銀河系の星々を見ると、太陽も銀河系内で「公転」しているようだ。

ならば、銀河系の中心は動かない？？

他にも銀河があって、互いの距離は変化している。

いったい何が止まっていて何が動いているの？？？

特殊相対論：そもそも、動かないのはこれだ、と主張することはできない。
絶対的に静止しているものはなく、相対的な運動しか意味がない。

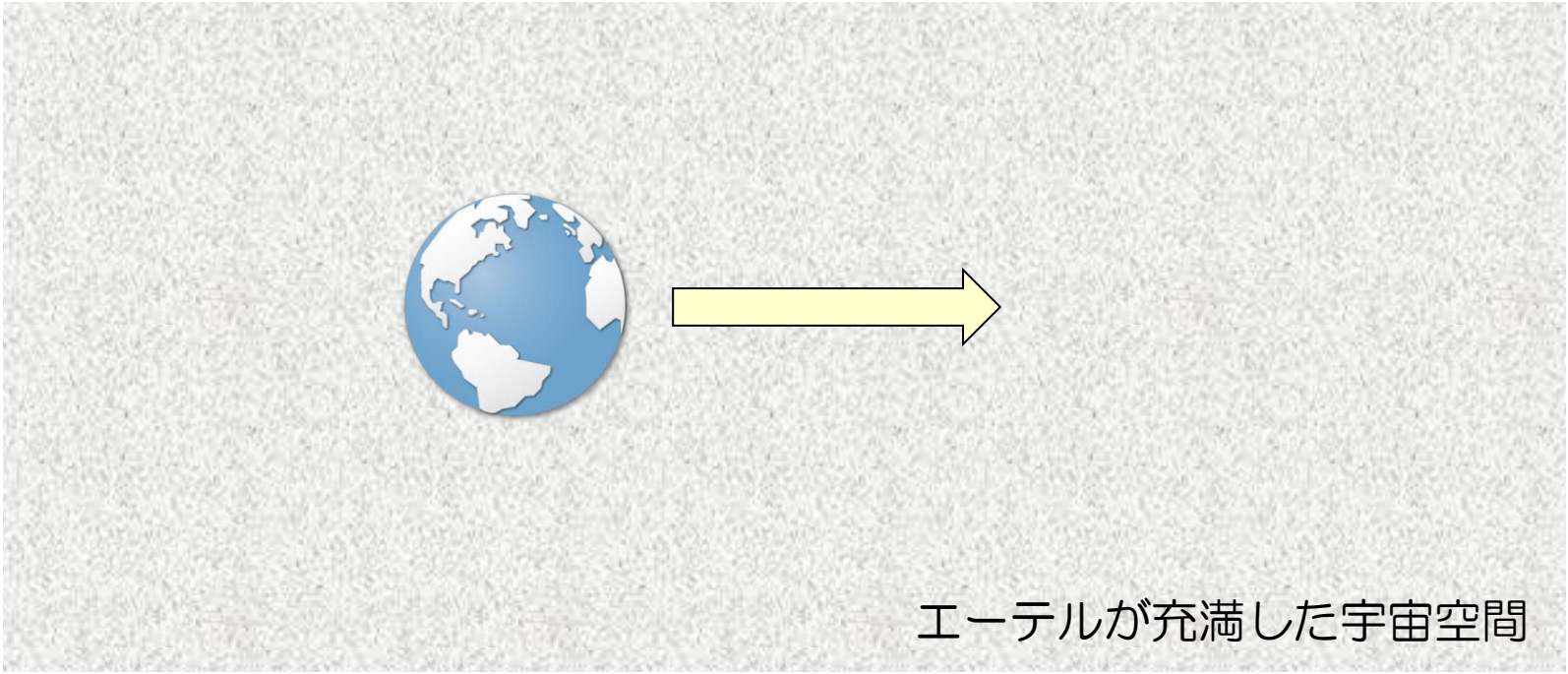
光エーテル説

（19世紀）

音は空気の振動が伝わる波動

↓

光も波動であるからには、何かの媒質（エーテル）が振動しているはず。



＊

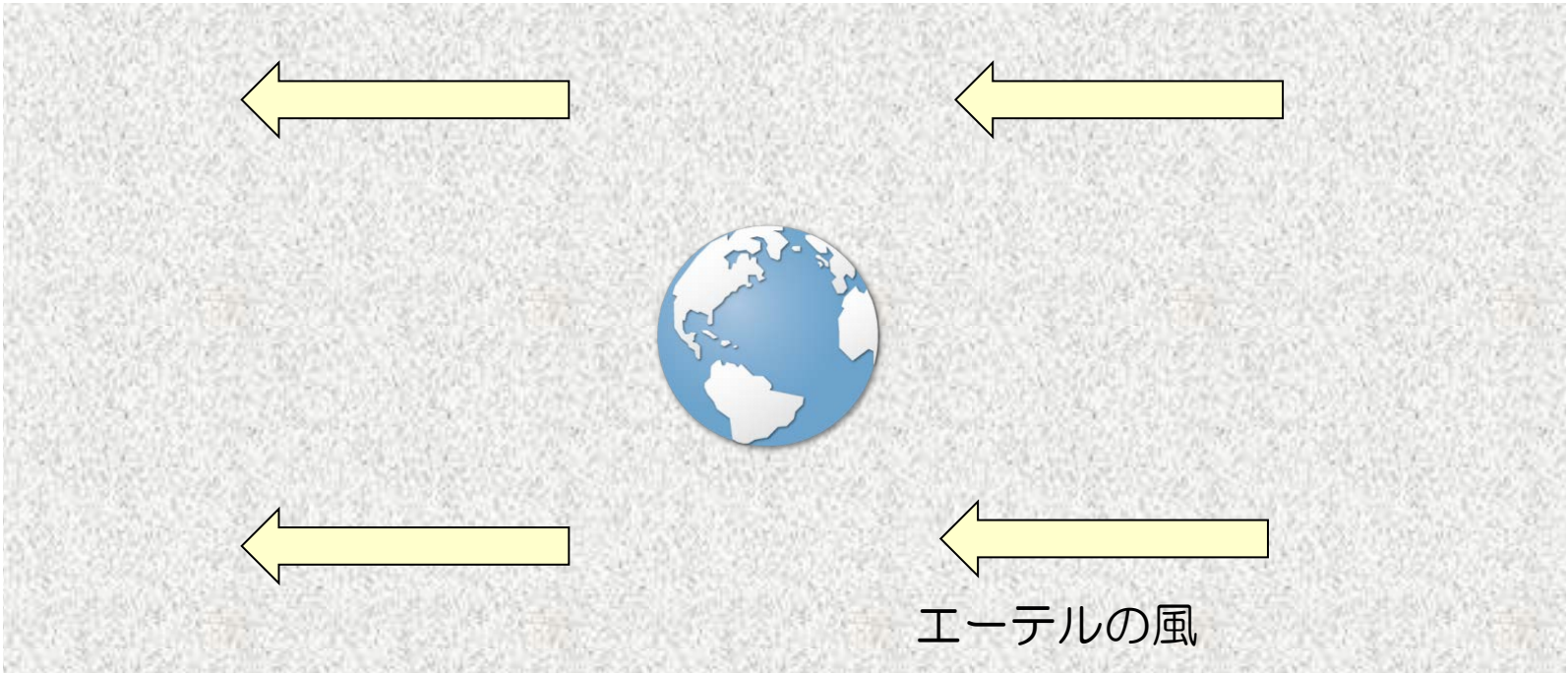
地球は、静止したエーテルの中を運動している。

イラスト出典：Siena
http://webdesignerdepot.com/2009/03/200-free-exclusive-icons-siena/

光エーテル説

（19世紀）

地球上で見ると、エーテル風と同方向の光はより速く進み、
エーテル風と逆方向の光はより遅く進むはずである。



＊

地球から見れば、エーテルが逆方向に動いている。

イラスト出典：Siena
http://webdesignerdepot.com/2009/03/200-free-exclusive-icons-siena/

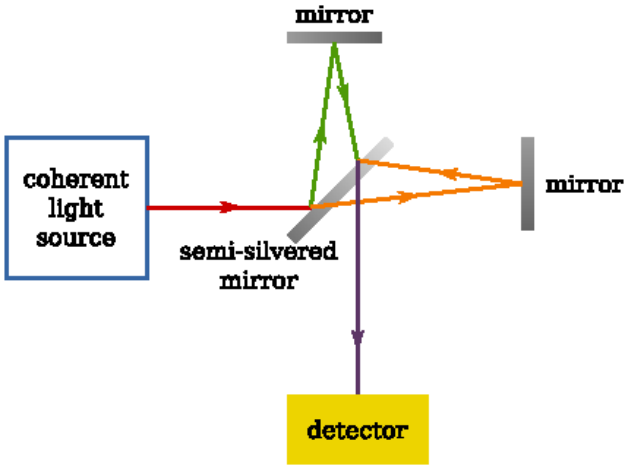
光エーテル説の否定

（19世紀）

地球上で見ると、エーテル風と同方向の光はより速く進み、
エーテル風と逆方向の光はより遅く進むはずである。

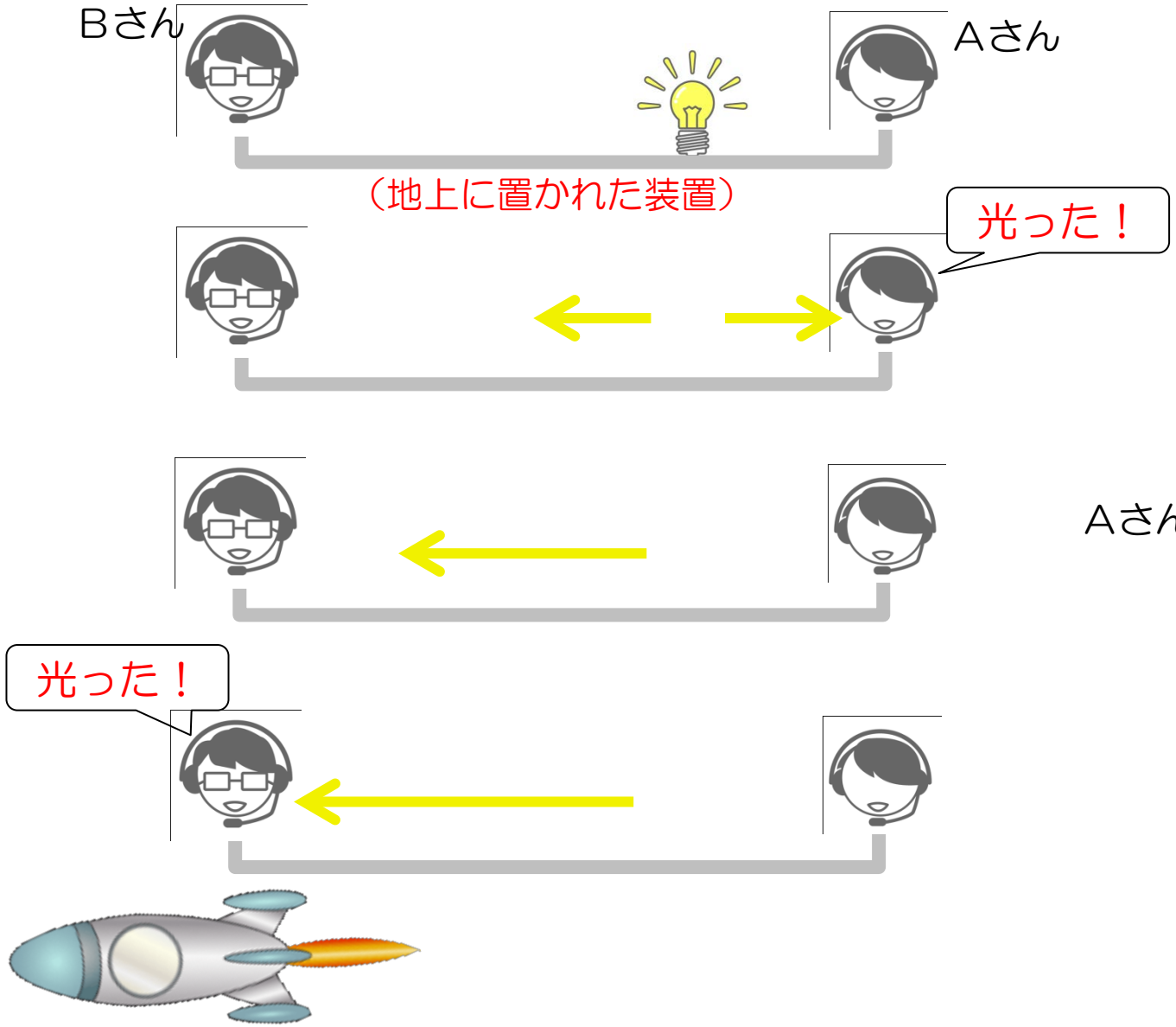
マイケルソンとモーリーの実験

方向による光速度の違いは検出されず。



アインシュタインの特殊相対論：エーテルの存在は考えない。
動いている人から見ても、真空中の光の速度は常に一定で、
物理法則は全く同じに見える。
自分が動いているか、静止しているかは、決めようがない。

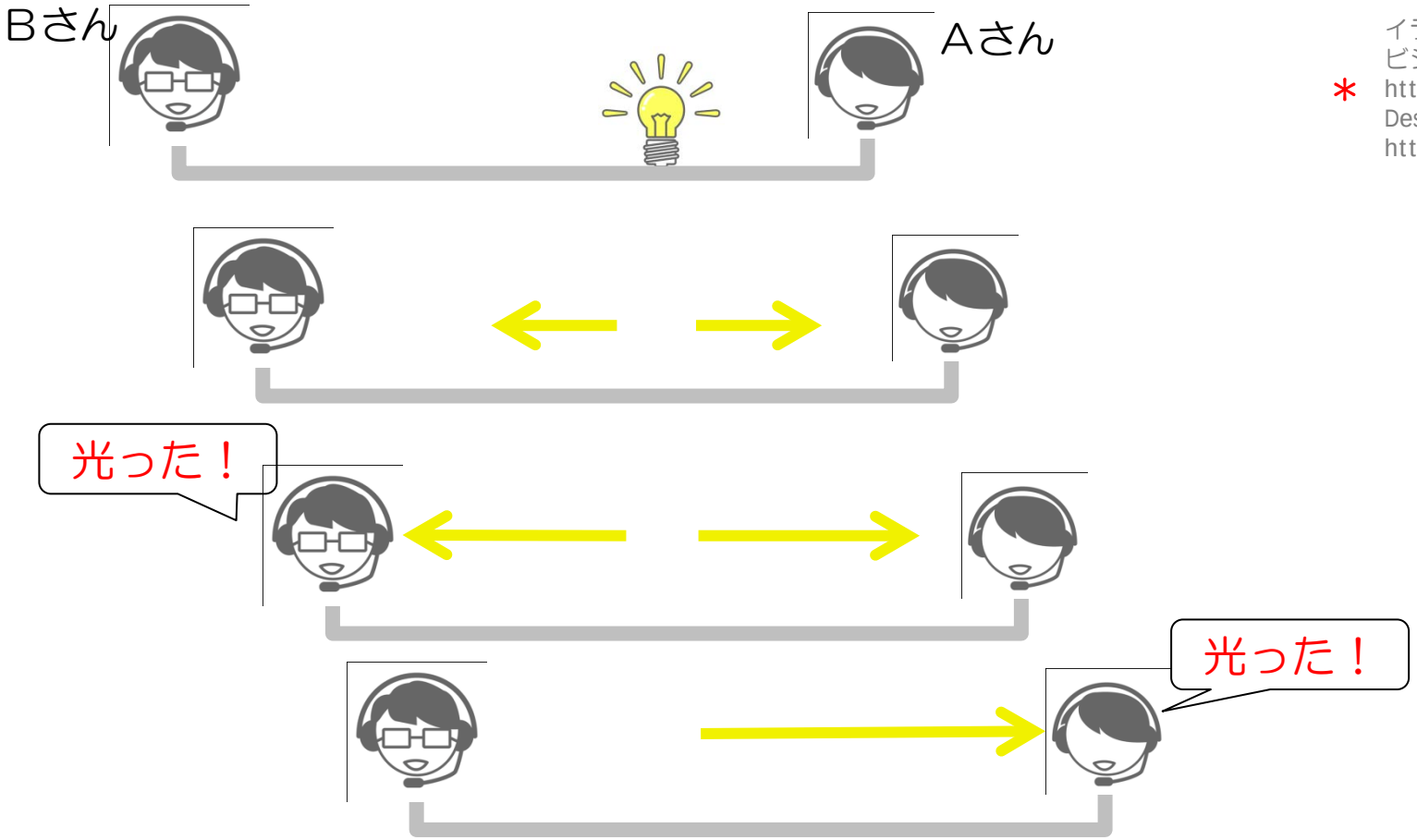
特殊相対性理論と同時性



イラスト出典：
ビジネスアイコン無料素材
＊ http://business-icon.com/
DesignBank
http://sozai-bank.com/

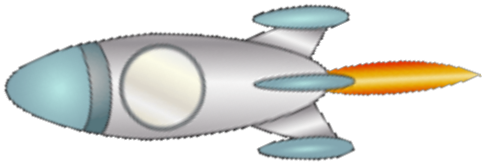
Aさんが先に光を見たと言う

特殊相対性理論と同時性



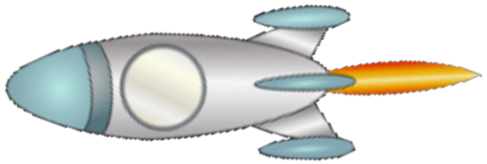
イラスト出典：
ビジネスアイコン無料素材
＊ http://business-icon.com/
DesignBank
http://sozai-bank.com/

ロケットから見ても、光の速度は常に一定



Bさんが先に光を見たと言う

特殊相対性理論と同時性



地上から見ていると、Aさんが先に光を見たと言う。

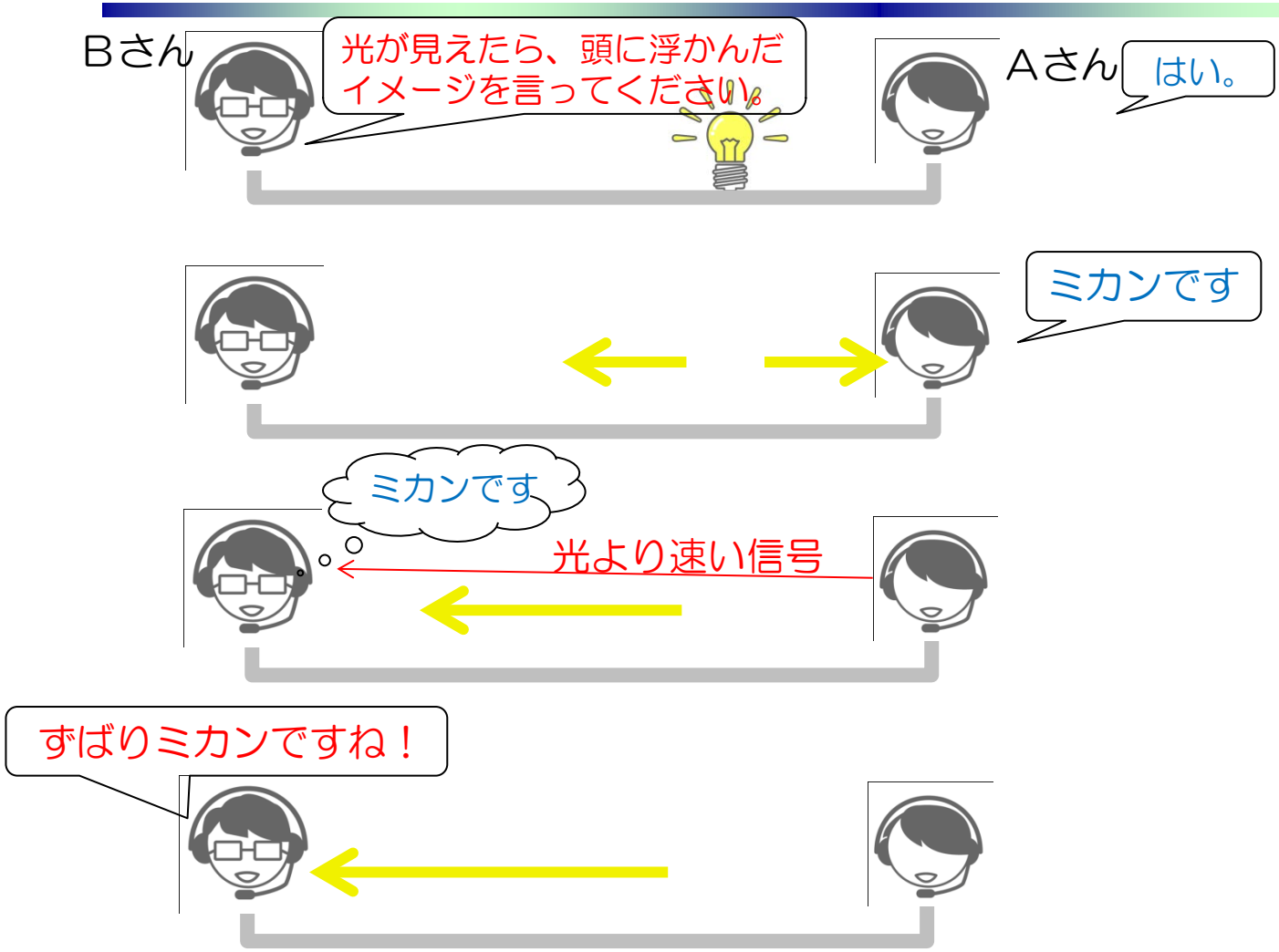
ロケットから見ていると、Bさんが先に光を見たと言う。

特殊相対論：どちらの言い分も正しい。

離れた２地点で起こる出来事が、たかだか（距離÷光速度）くらいの時間だけずれている場合、見る立場によって、順序は変わってしまう。

本当はどちらが先か、などと議論しても意味がない。

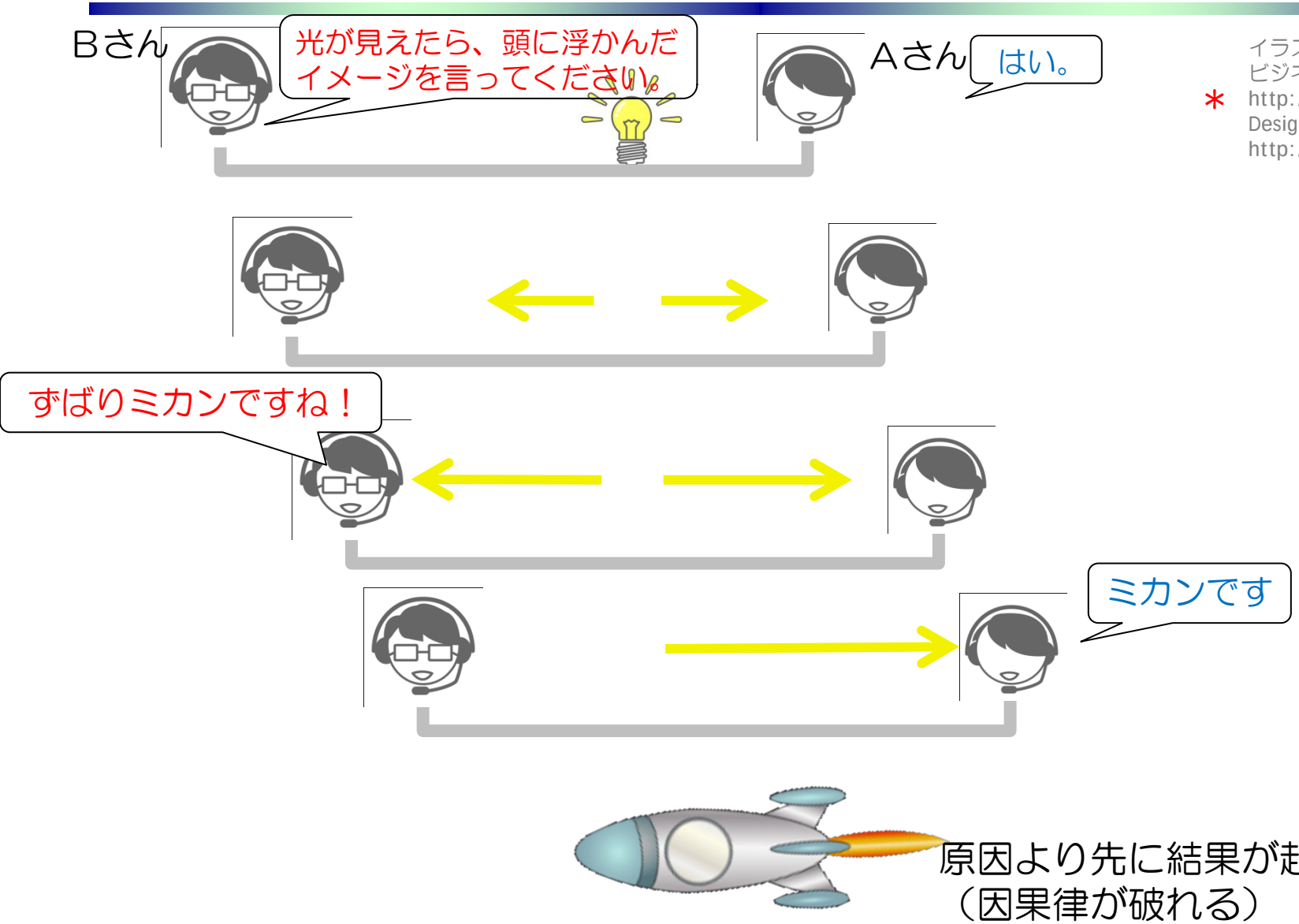
超光速通信と因果律



イラスト出典：
ビジネスアイコン無料素材
＊ http://business-icon.com/

超光速の通信が出来ると・・・

超光速通信と因果律



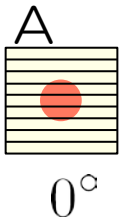
イラスト出典：
ビジネスアイコン無料素材
＊ http://business-icon.com/
DesignBank
http://sozai-bank.com/

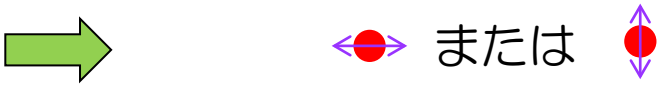
原因より先に結果が起きてしまう
（因果律が破れる）

光子対と偏光フィルター

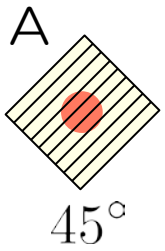
Aの光子に置いたフィルター

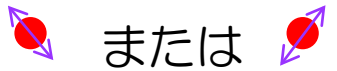
実験結果の示す
Bの光子の偏光





見る立場によっては、
Aのフィルターを置く前に、Bの光子の偏光が先に変化してしまう。
（因果律が破れるように見える）

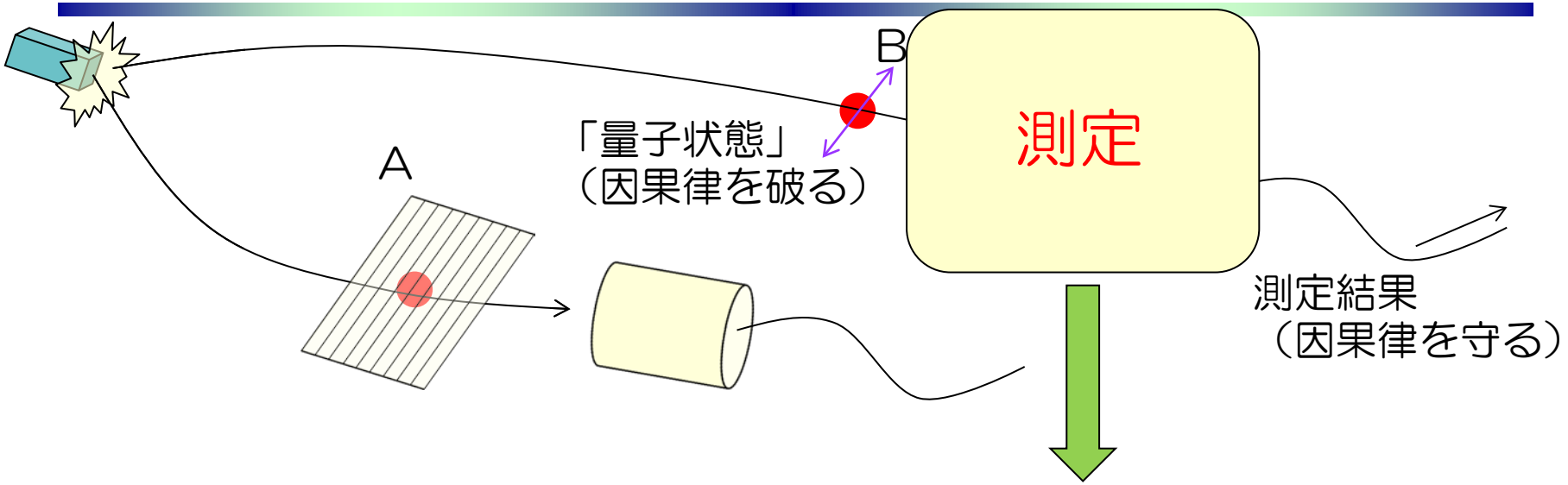




「光子の偏光」という概念を捨てていろいろ工夫しても、この不自然さを解消することはできない（ベルの不等式の破れ：前回の話）

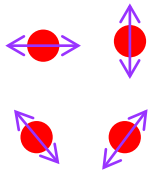
量子力学では、
この光子の偏光方向のことを、
「量子状態」、あるいは、「状態ベクトル」、「波動関数」
などと呼び、測定結果はこの量子状態に応じて確率的に決まると考える。

量子力学における測定



測定できることが限られている。

なんでもかんでも好きな精度で
測定できるわけではない。

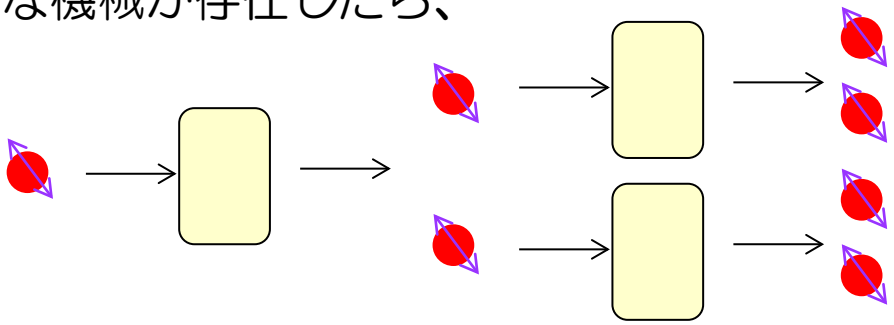
例えば、  の４種類を正確に見分ける測定はできない
（測定結果が因果律を破ってしまう）

量子力学が正しい限りは、どんなに技術が進んでも、
決してできない禁止事項が存在する。(No-go theorems)

量子力学における禁止事項

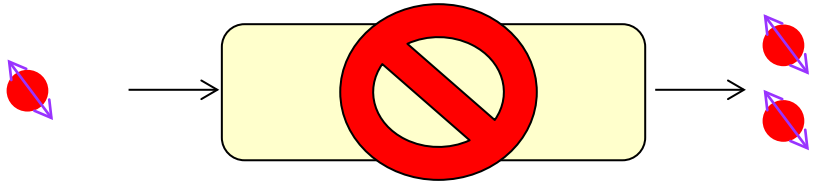
いろいろな量子状態の複製を作る機械は存在しない（No-cloning 定理）。

そんな機械が存在したら、

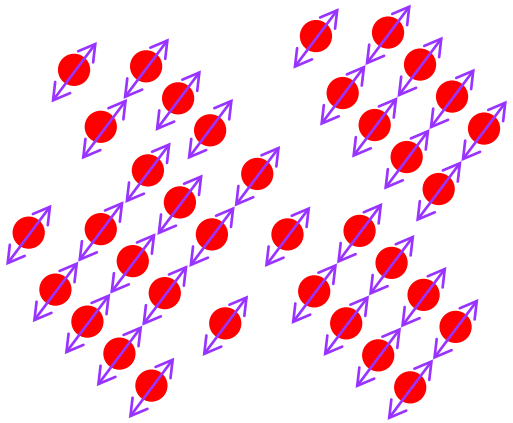


同じ偏光を持つ光子を無数に作れる。
すると、偏光方向が良い精度で決定出来てしまう。

任意の偏光の１光子をもらい、同じ偏光を持つ光子のコピーを作る機械は存在しない



光子の偏光方向を測る



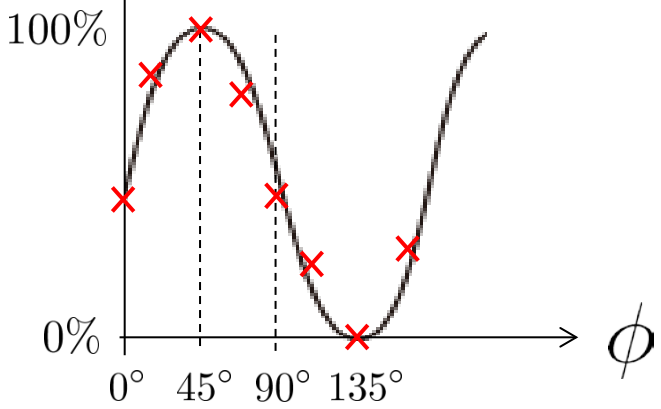
測定によって偏光方向を
悪くない精度で決定できる。

ϕ

$\phi = 0$ 45 $\phi = 90$

同じ偏光の光子をたくさん用意して、透過した個数の割合を測定

透過した割合



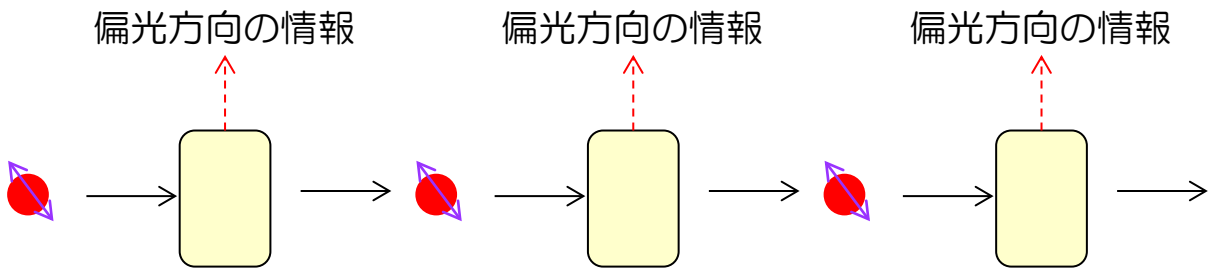
確率現象なので、誤差が生じる

N 個測ると相対誤差が
だいたい $1/\sqrt{N}$ 程度

量子力学における禁止事項

光子の偏光方向に影響を与えずに、偏光方向についての手掛かりを得ることはできない。

そんな方法が存在したら、

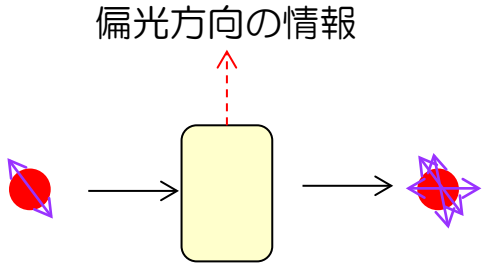


繰り返し適用すればどんどん情報が蓄積され、良い精度で偏光方向がわかってしまう。

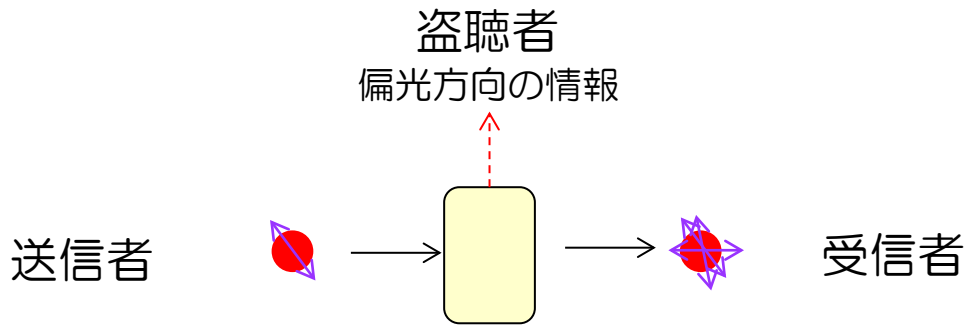
量子状態から情報を引き出そうとすると、状態はその影響を受けて乱される（もとの状態から変化する）。

“Information-disturbance trade-off”

量子力学が正しい限りは、どんなに技術が進んでも、この制約からは逃れられない。



暗号通信への応用

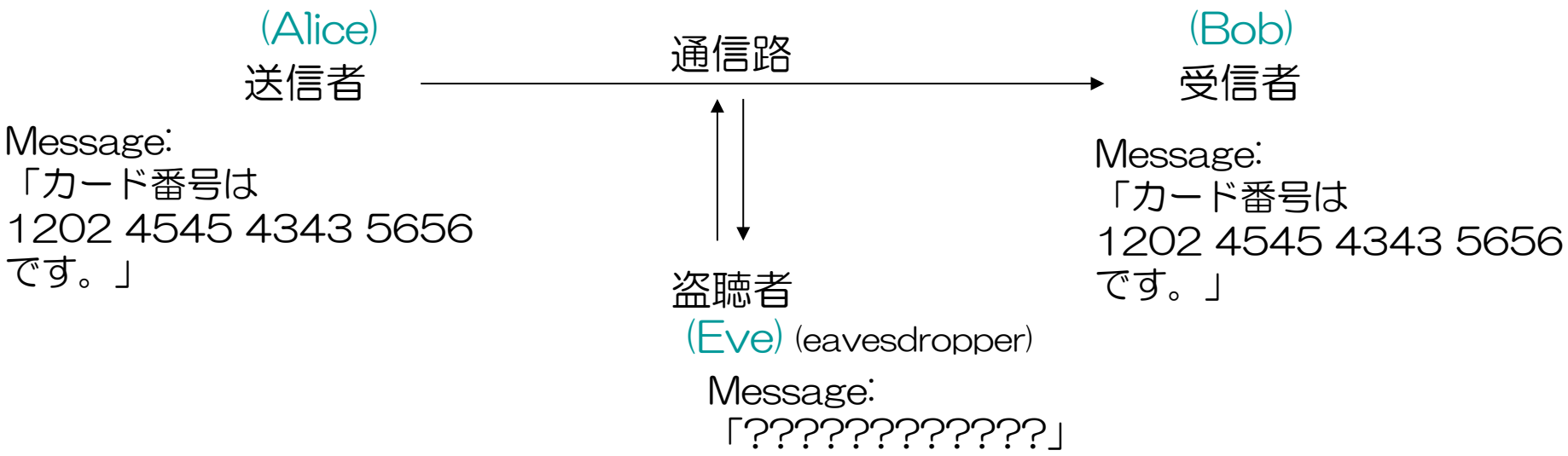


光子の偏光に情報を載せて送る。

Eveが情報を盗み見たら、偏光が変化するので、
それをBobがチェックすれば、見られたことがわかるはず。

量子力学が正しい限りは、どんなに技術が
進んでも、この制約からは逃れられない。

暗号の目的


(Alice)
送信者
通信路
(Bob)
受信者
Message:
「カード番号は
1202 4545 4343 5656
です。」
Message:
「カード番号は
1202 4545 4343 5656
です。」
盗聴者
(Eve) (eavesdropper)
Message:
「???????????????」

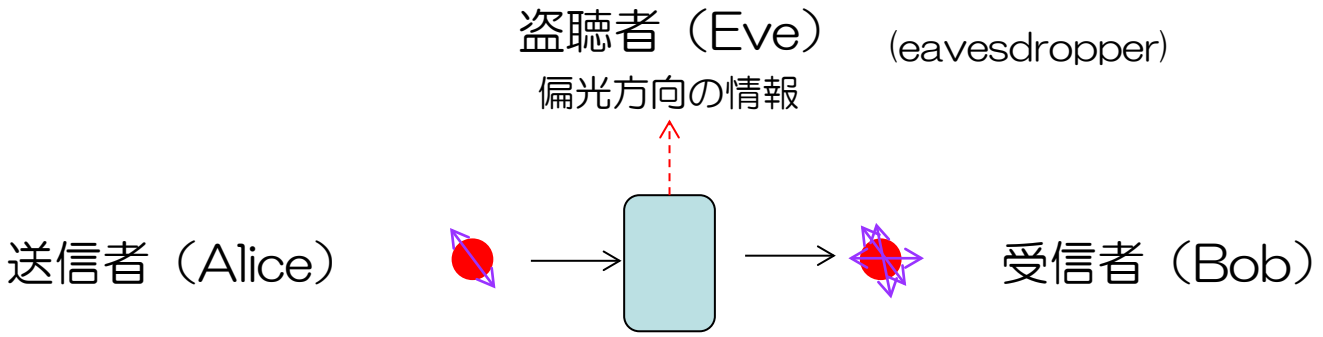
普通の暗号

情報理論的には、Eveに分からないようにMessageを送ることはできない。
（符号化方法が公開されていれば、原理的には復号化可能）
（符号化方法を秘密にしても、繰り返すうちにいずれ露見する。）

計算量論的には可能：Bobはたやすく解読できるが、
Eveが解読するには難しい計算が必要

・ ５０年間秘密にしたければ、５０年後の計算機の技術を予想しなければならない。
・ 計算の難しさを厳密に保証する理論が未完成。

暗号通信への応用



光子の偏光に情報を載せて送る。

Eveが情報を盗み見たら、偏光が変化するので、
それをBobがチェックすれば、見られたことがわかるはず。

量子力学が正しい限りは、どんなに技術が進んでも、この制約からは逃れられない。

そもそもBobに情報が確実には伝わらないのでは？

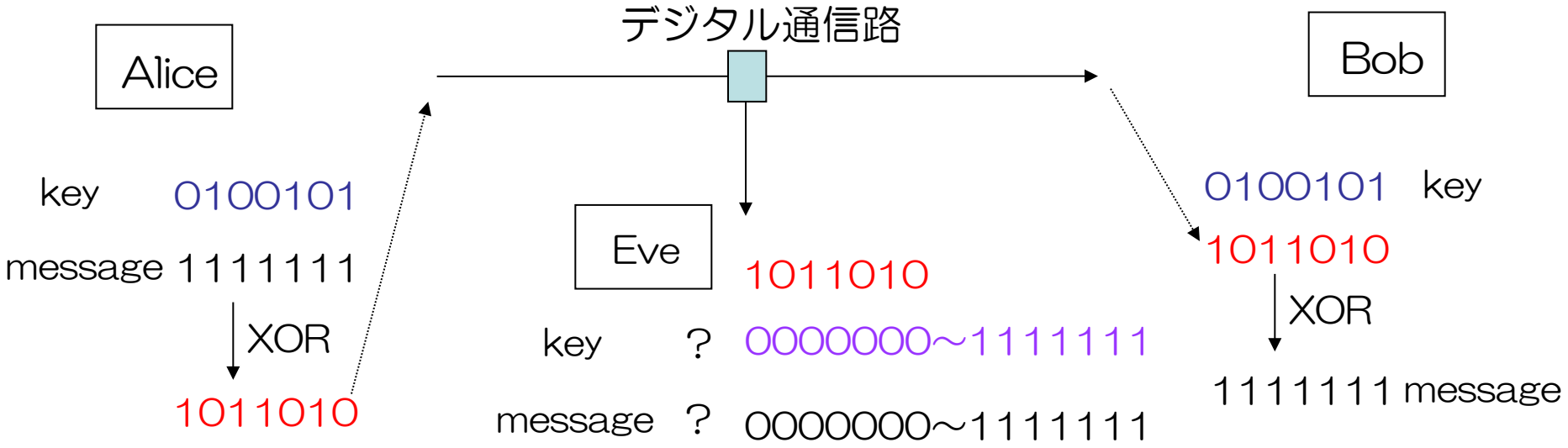
見られたことが後でわかってもあとの祭りでは？

このような問題を解決して暗号通信を行う仕組みが量子暗号（量子鍵配送）。

ワンタイムパッド

秘密鍵(secret key)：
AliceとBobに共有されたランダムなビット列で、Eveはその内容を知らない。

AliceとBobが秘密鍵を持っていると、古くから知られた方法で
同じ長さのmessageを安全に送れる。



秘密鍵は使い捨て
秘密鍵の増幅は不可

そもそも秘密鍵をどうやってAliceとBobに配るのか？

量子暗号

秘密鍵(secret key)：
AliceとBobに共有されたランダムなビット列で、Eveはその内容を知らない。

ワンタイムパッド

AliceとBobが秘密鍵を持っていると、古くから知られた方法で同じ長さのmessageを安全に送れる。

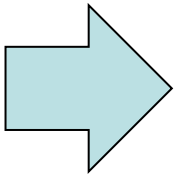
そもそも秘密鍵をどうやってAliceとBobに配るのか？

光子の通信

光子の偏光に情報を載せて送ると、見られたことがわかるはず。

そもそもBobにも情報が確実には伝わらないのでは？

見られたことが後でわかってもあとの祭りでは？



ランダムなビット列の情報を光子の偏光に載せて送り、Eveに見られなかったと確認できたものを秘密鍵として採用（量子鍵配送）。

そうやって作った秘密鍵を用い、ワンタイムパッドでmessageを送る。

量子暗号

秘密鍵(secret key)：
AliceとBobに共有されたランダムなビット列で、Eveはその内容を知らない。

ワンタイムパッド

AliceとBobが秘密鍵を
同じ長さのmessageを

そもそも秘密鍵

ランダムなビット列

０１００１０１１０１０

Ｘ　　ＸＸ　　Ｘ

１００１１００

ランダムなビット列

光子の通信

光子の偏光に情報を載せて送ると、見られたことがわかるはず。

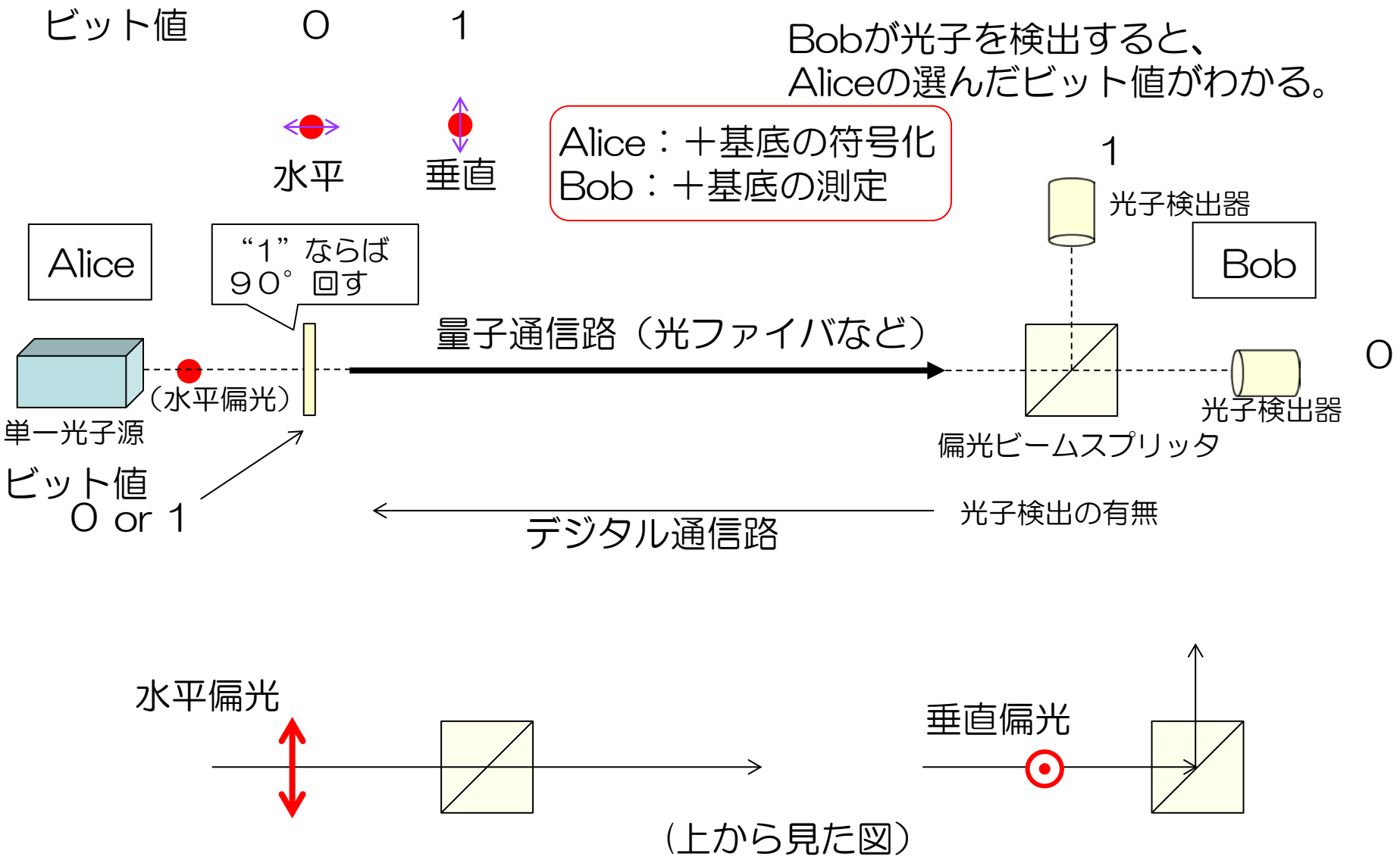
そもそもBobにも情報が確実には伝わらないのでは？

見られたことが後でわかってもあとの祭りでは？

ランダムなビット列の情報を光子の偏光に載せて送り、Eveに見られなかったと確認できたものを秘密鍵として採用（量子鍵配送）。

そうやって作った秘密鍵を用い、ワンタイムパッドでmessageを送る。

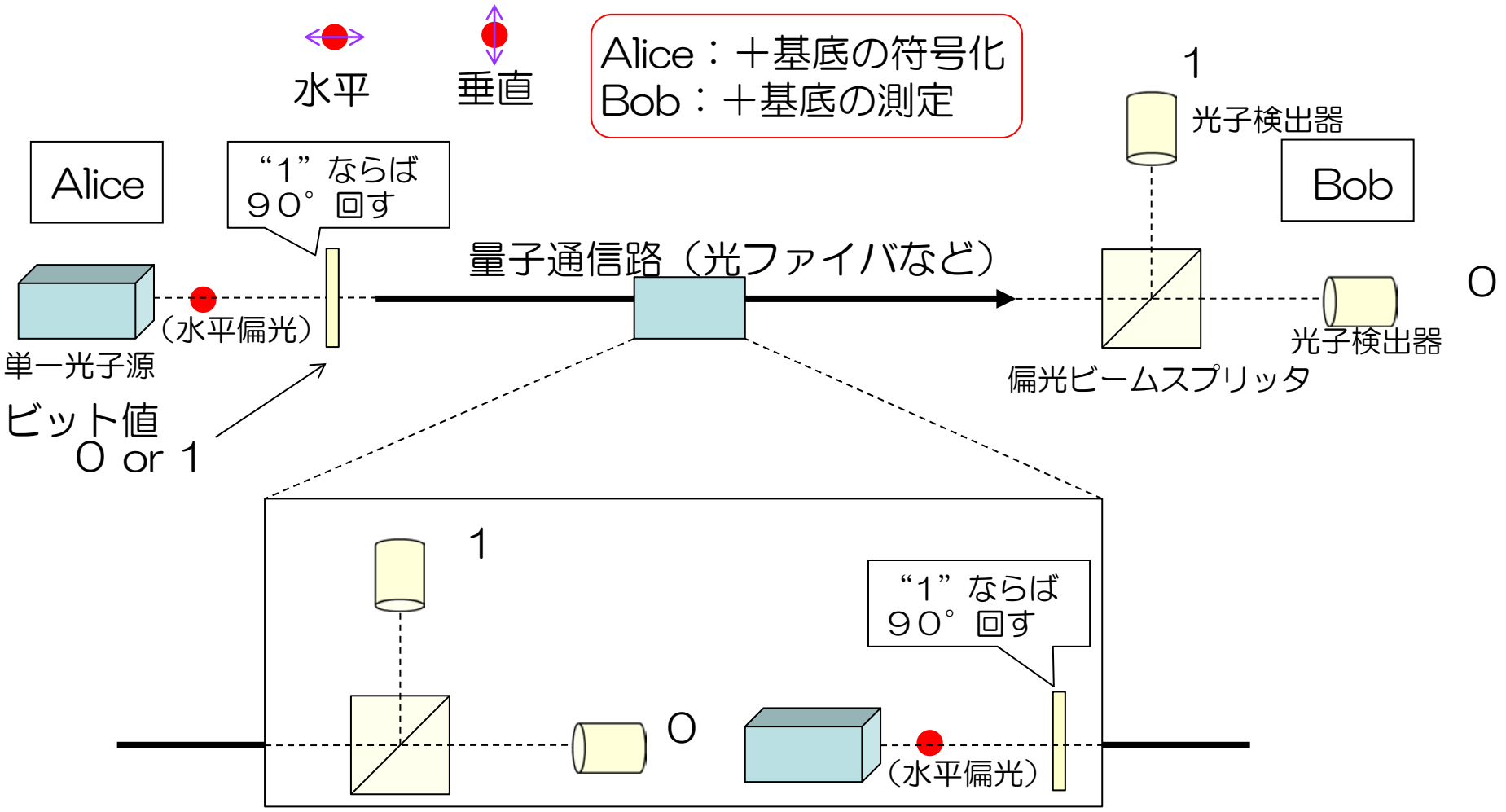
光子の偏光に情報を載せる



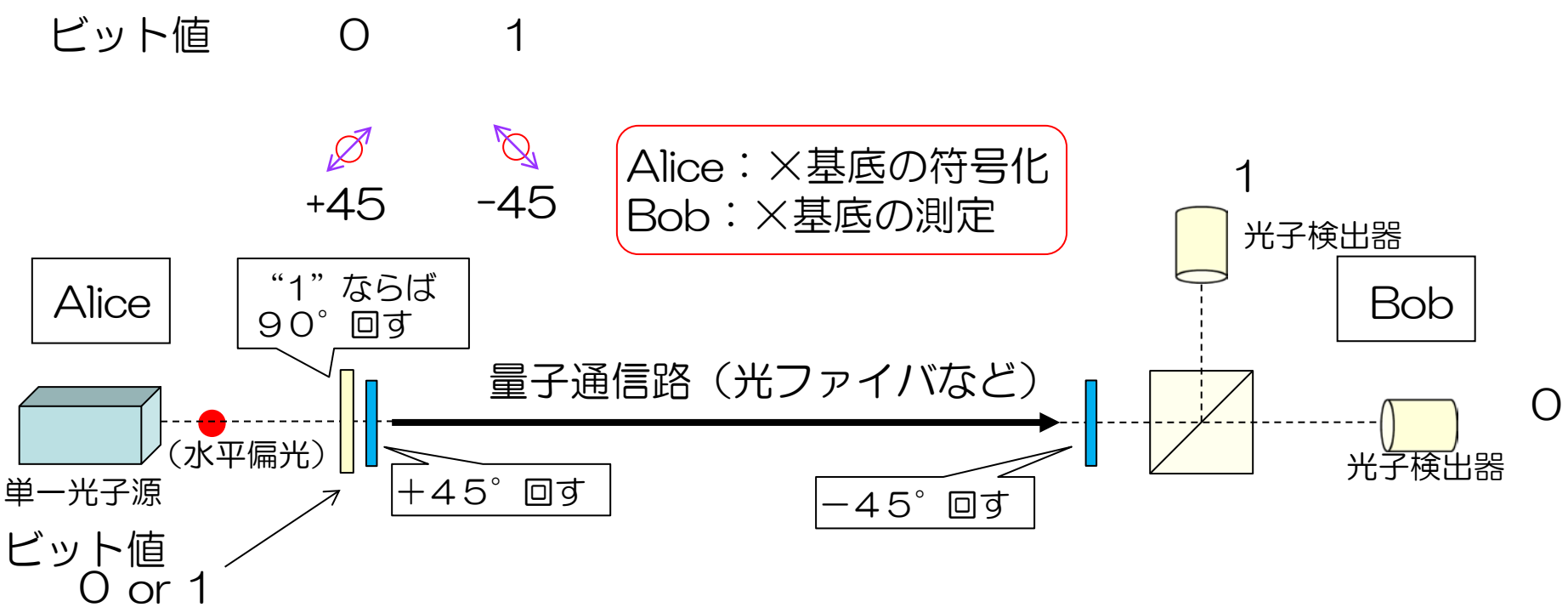
光子の偏光に情報を載せる

ビット値　　0　　1

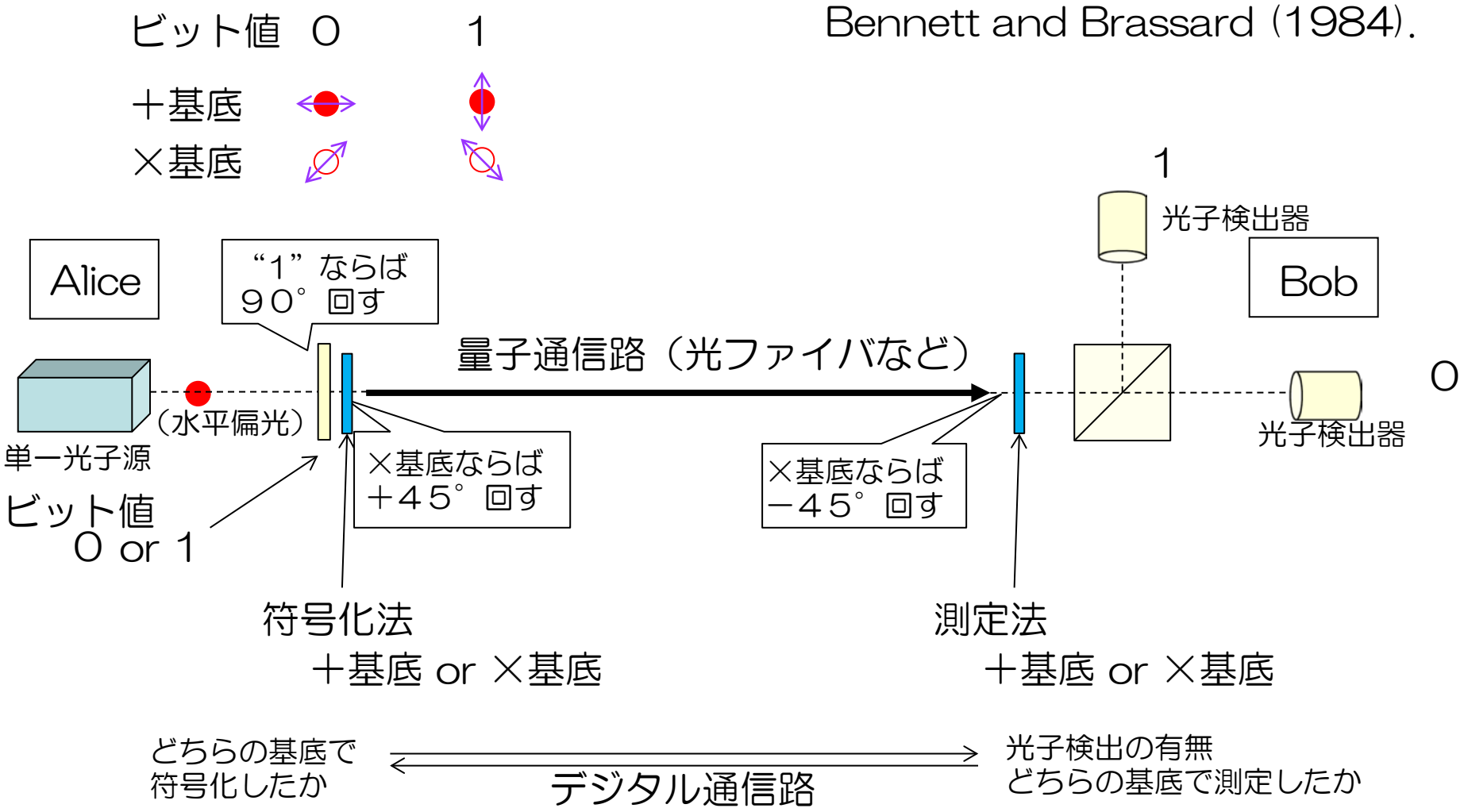
ランダムなビット列を共有できるが、
Eveに盗聴されても痕跡は残らない。



情報を載せる別のやり方

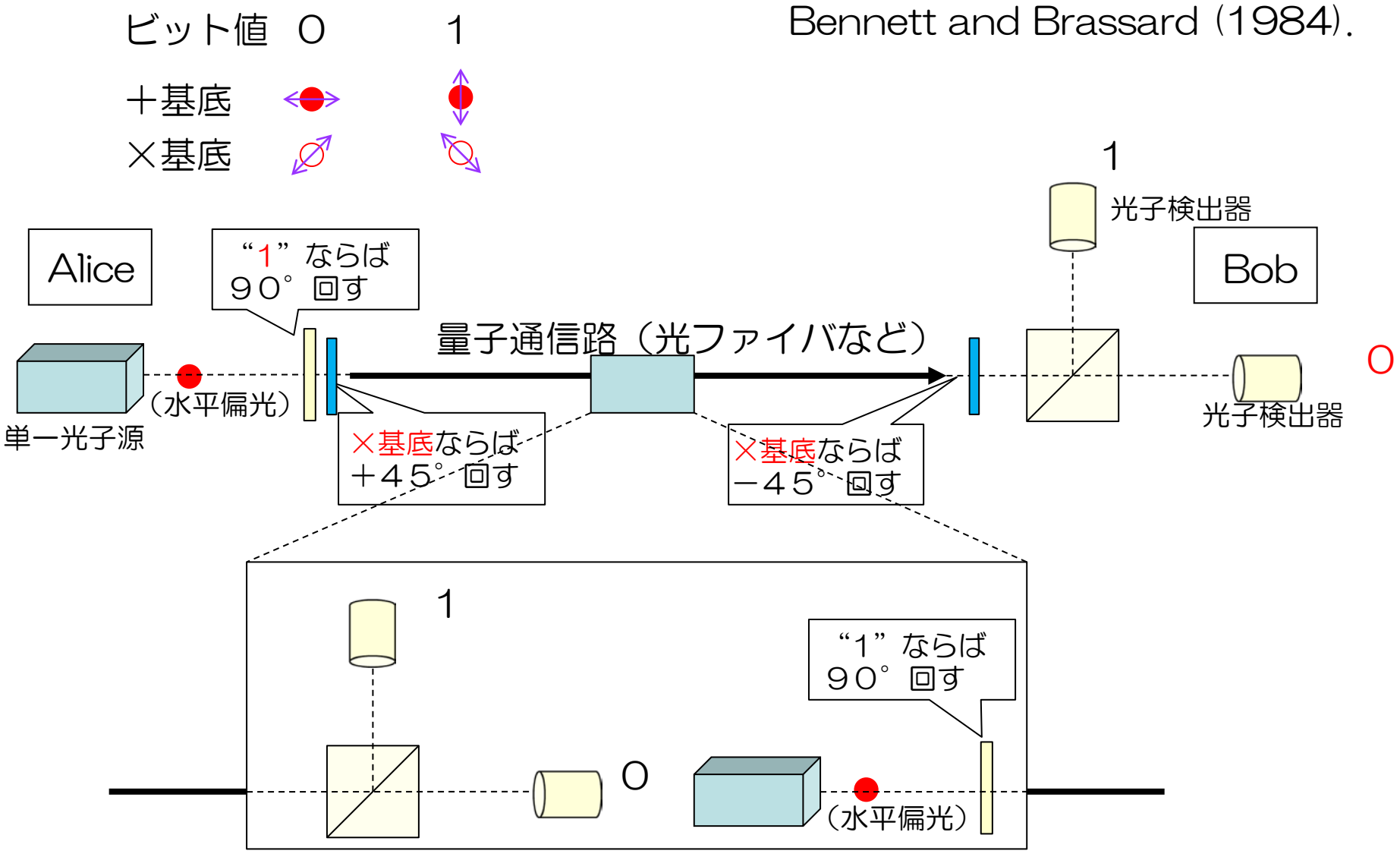


ＢＢ８４量子鍵配送方式

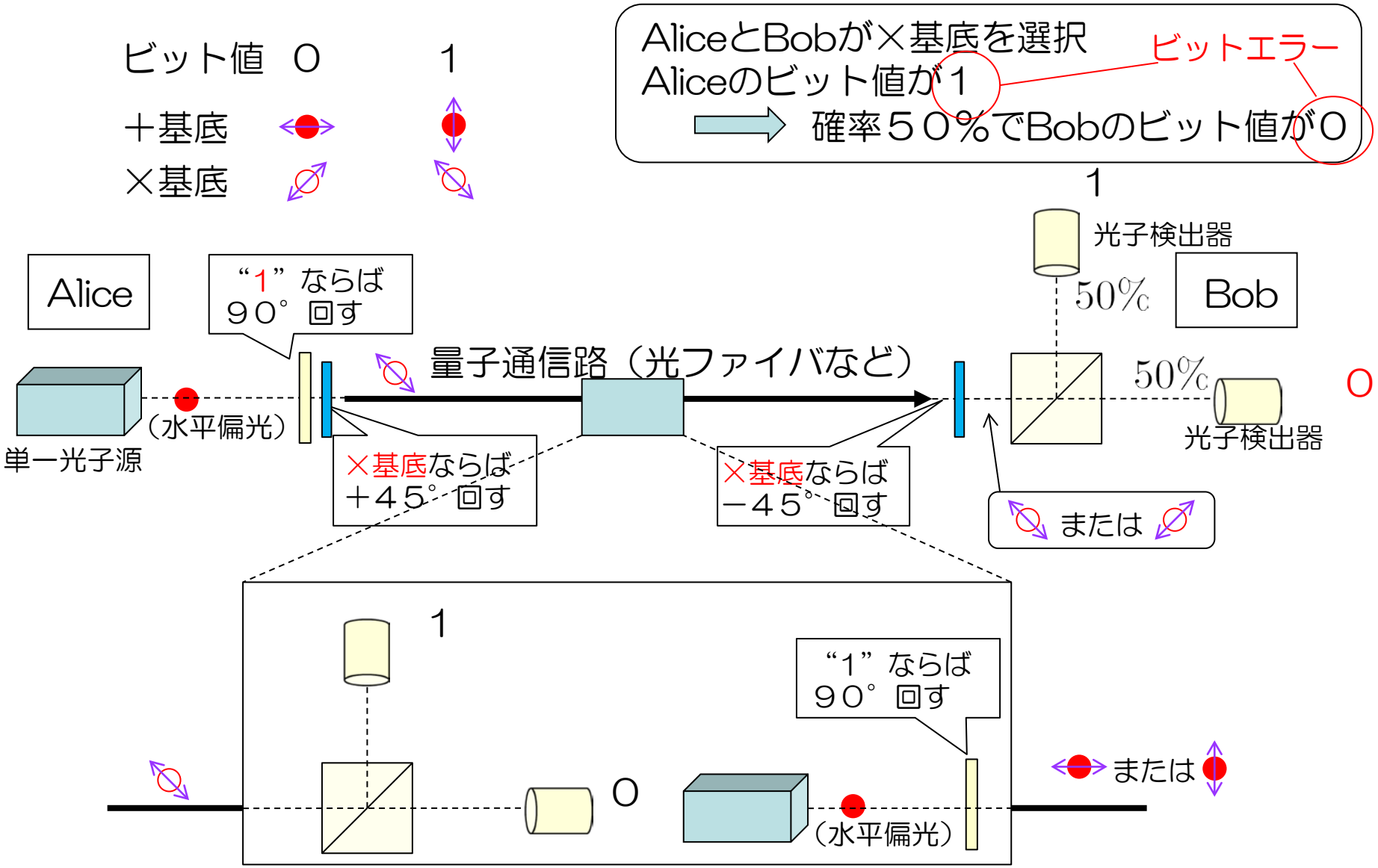


検出がなかったり、基底が不一致の場合は失敗とみなす。
これを繰り返せば、ランダムなビット列を共有できる。

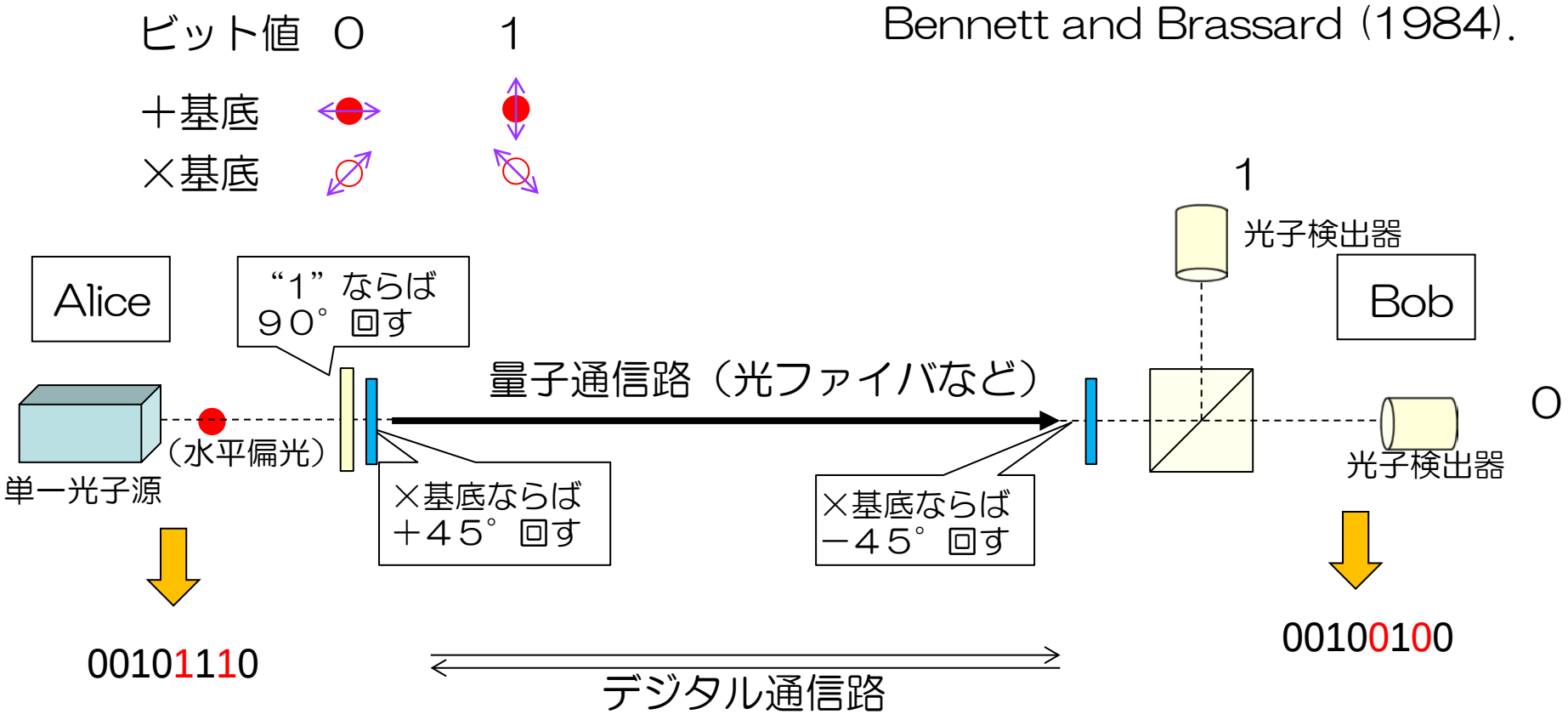
盗聴があると・・・


ビット値　0　1
Bennett and Brassard (1984).
＋基底
×基底
1
光子検出器
Alice
“1” ならば
９０° 回す
Bob
量子通信路（光ファイバなど）
0
（水平偏光）
単一光子源
×基底ならば
＋４５° 回す
×基底ならば
－４５° 回す
光子検出器
1
“1” ならば
９０° 回す
0
（水平偏光）

盗聴があると・・・


ビット値　0　1
＋基底
×基底
AliceとBobが×基底を選択
Aliceのビット値が1
確率５０％でBobのビット値が0
ビットエラー
1
光子検出器
50%
Bob
Alice
“1”ならば
９０°回す
量子通信路（光ファイバなど）
50%
0
（水平偏光）
単一光子源
光子検出器
×基底ならば
＋４５°回す
×基底ならば
－４５°回す
または
1
“1”ならば
９０°回す
または
0
（水平偏光）

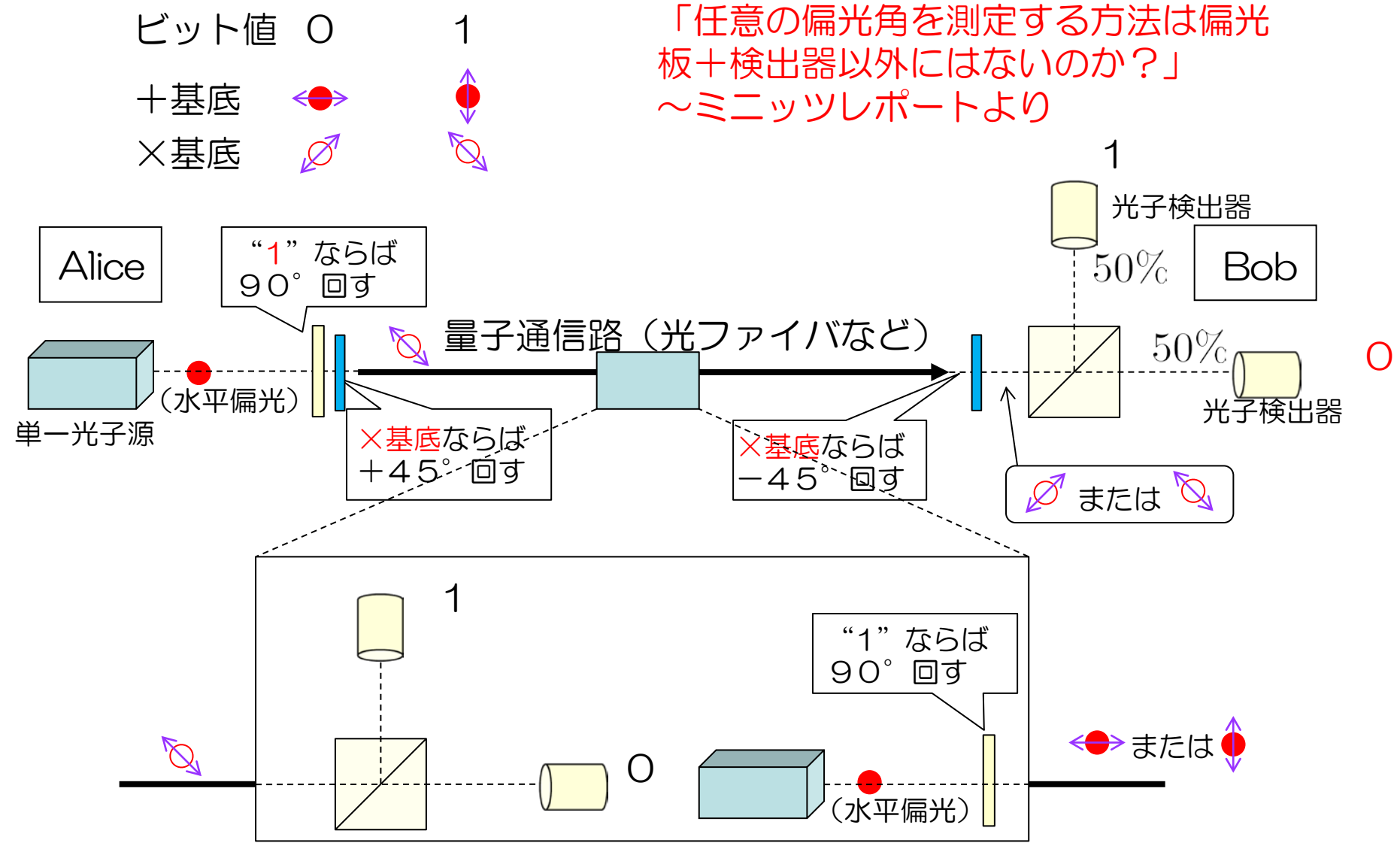
盗聴の有無をチェック



ビットの場所をランダムにいくつか選び（ランダムサンプリング）
ビット値の答え合わせをする。（そのビットは捨ててしまう。）

ビットエラーが見つかったら、盗聴されているので、全部捨てて、
秘密鍵としては採用しない。

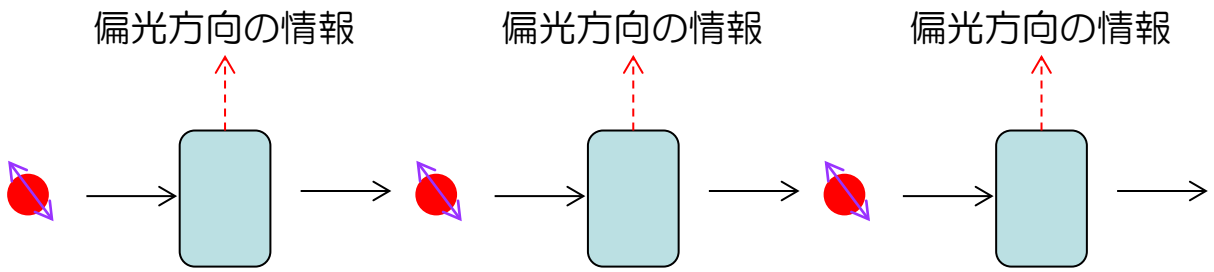
もっと高度な盗聴法は？


ビット値　0　1
＋基底
×基底
「任意の偏光角を測定する方法は偏光板＋検出器以外にはないのか？」
～ミニッツレポートより
1
光子検出器
Alice
“1”ならば
90°回す
50%
Bob
量子通信路（光ファイバなど）
50%
0
（水平偏光）
単一光子源
×基底ならば
＋45°回す
×基底ならば
－45°回す
光子検出器
または
1
“1”ならば
90°回す
または
0
（水平偏光）

量子力学における禁止事項

光子の偏光方向に影響を与えずに、偏光方向についての手掛かりを得ることはできない。

そんな方法が存在したら、

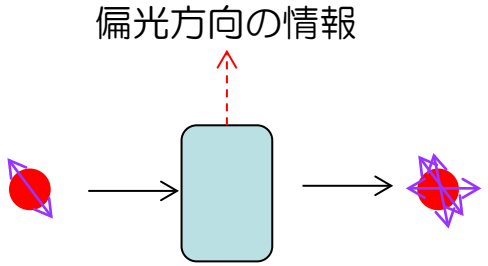


繰り返し適用すればどんどん情報が蓄積され、良い精度で偏光方向がわかってしまう。

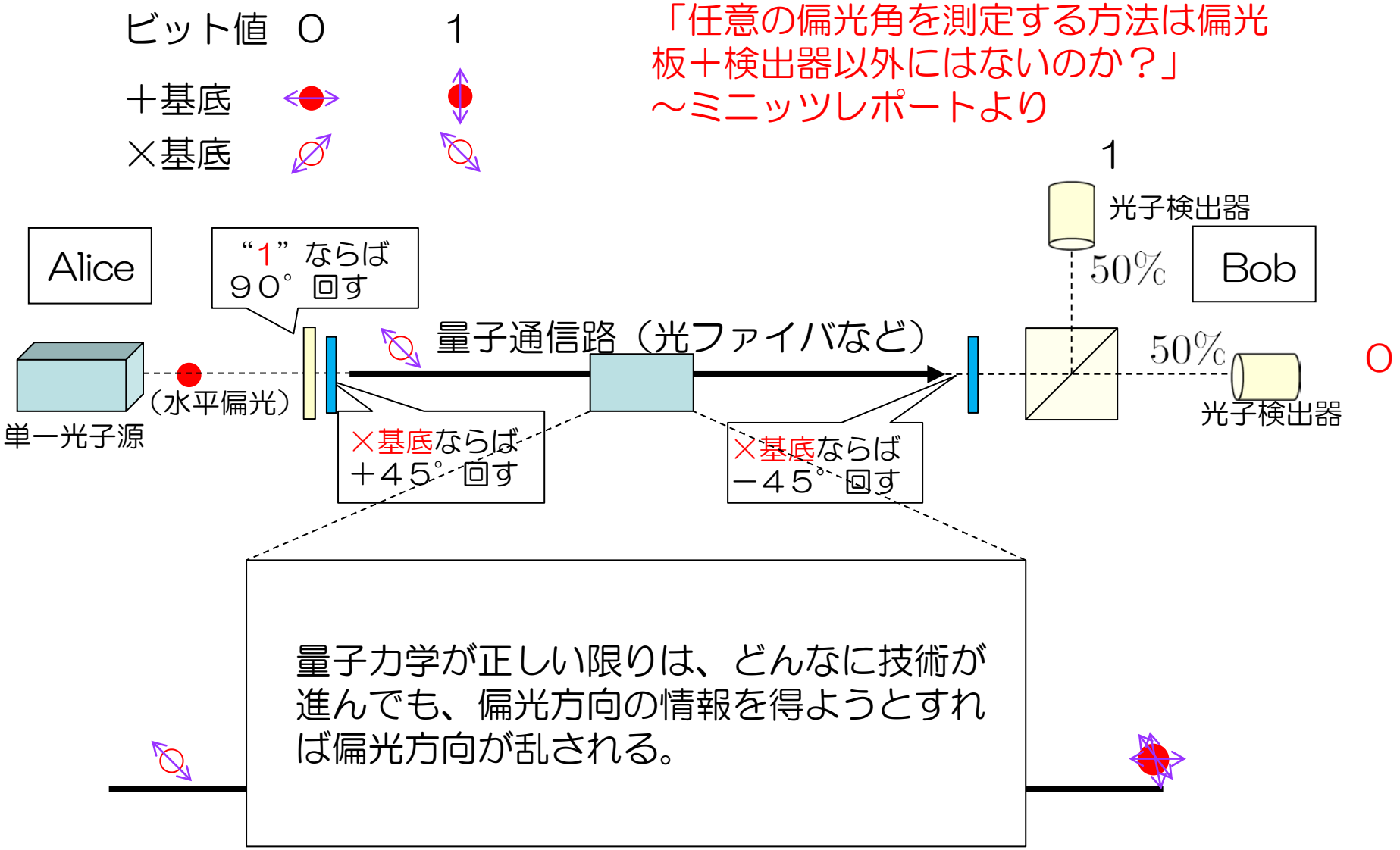
量子状態から情報を引き出そうとすると、状態はその影響を受けて乱される（もとの状態から変化する）。

“Information-disturbance trade-off”

量子力学が正しい限りは、どんなに技術が進んでも、この制約からは逃れられない。



もっと高度な盗聴法は？

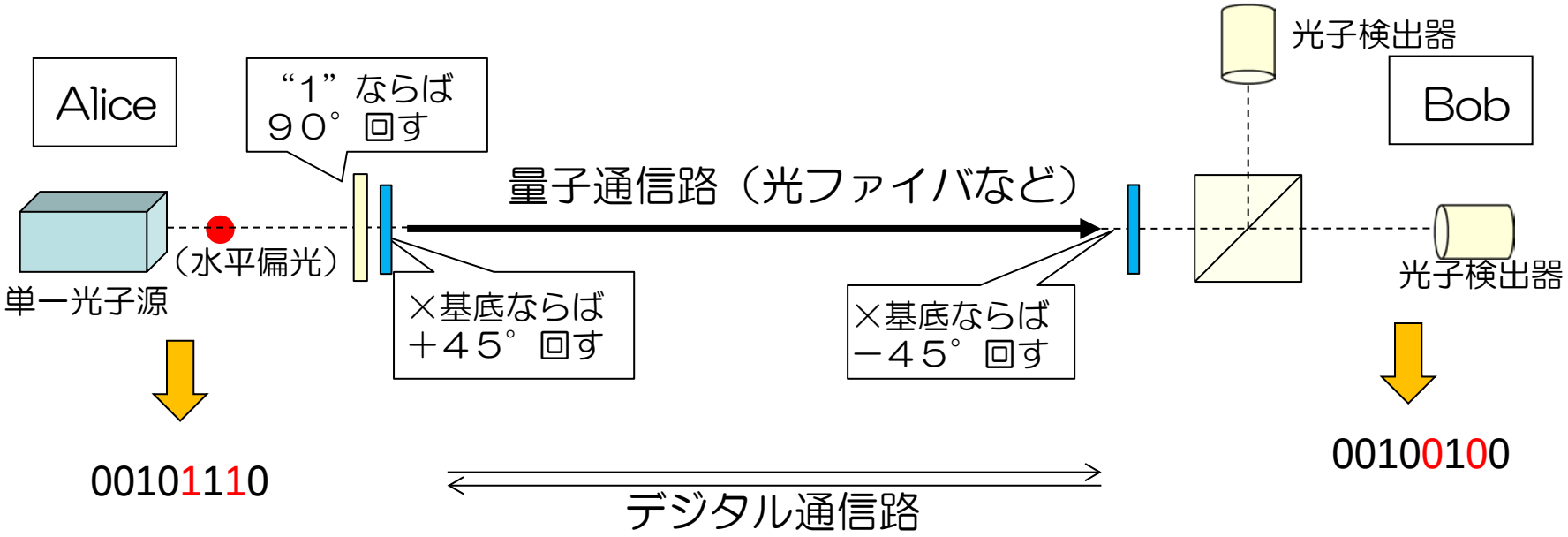

ビット値　0　1
＋基底
×基底
「任意の偏光角を測定する方法は偏光板＋検出器以外にはないのか？」
～ミニッツレポートより
1
光子検出器
Alice
“1”ならば
９０°回す
50%
Bob
量子通信路（光ファイバなど）
50%
0
（水平偏光）
単一光子源
×基底ならば
＋４５°回す
×基底ならば
－４５°回す
光子検出器
量子力学が正しい限りは、どんなに技術が進んでも、偏光方向の情報を得ようとすれば偏光方向が乱される。

盗聴の程度を監視する

ビットエラーが見つかったら、盗聴されているので、全部捨てて、秘密鍵としては採用しない。

この方法は問題あり！

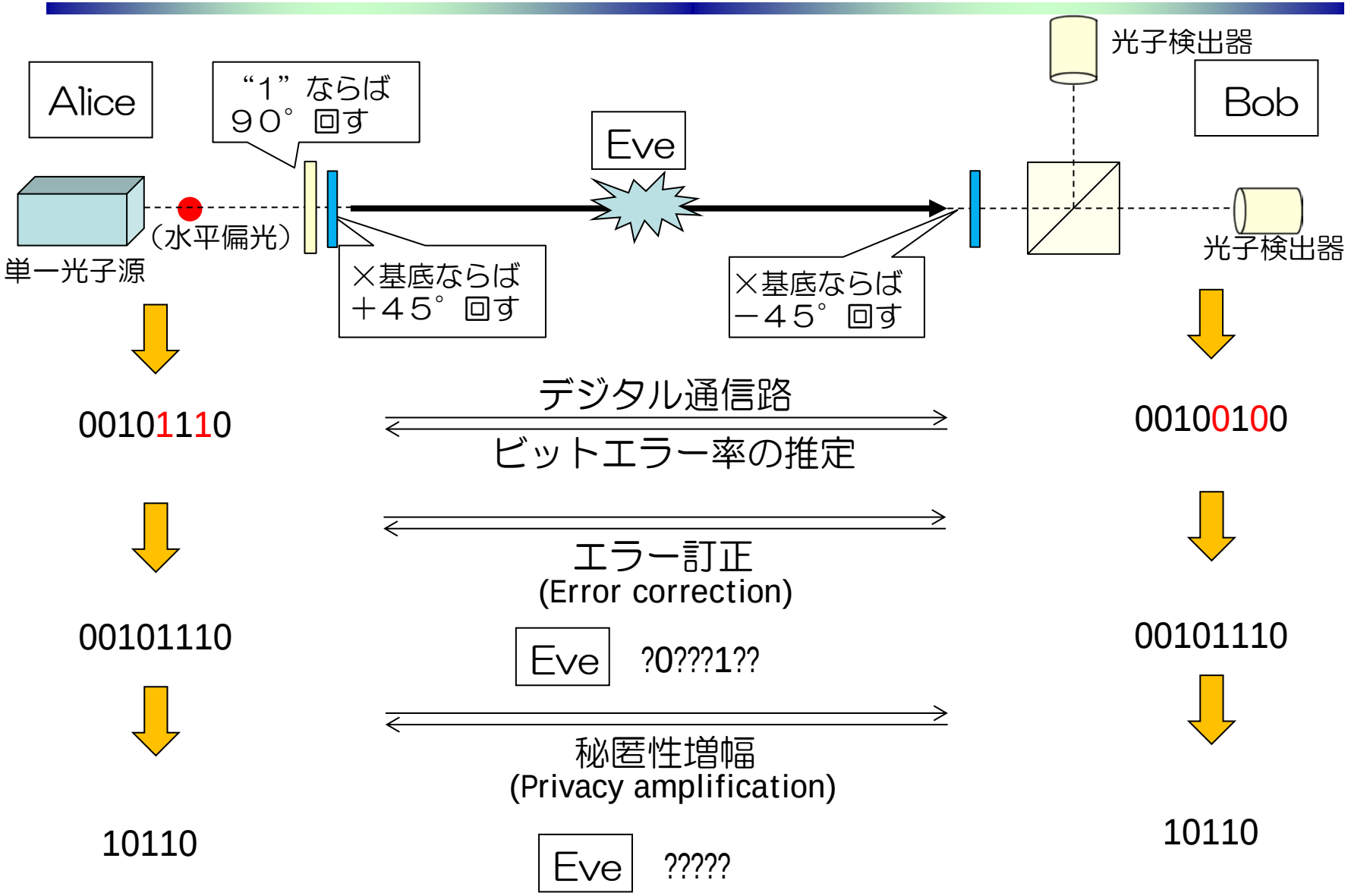
- 一部のビットしか盗聴しない場合、盗聴が発覚しない場合もある。
- 現実には、装置や通信路の不具合で盗聴がなくてもビットエラーがある。



ビットの場所をランダムにいくつか選び（ランダムサンプリング）
ビット値の答え合わせをする。（そのビットは捨ててしまう。）

その結果から、ビットエラーの生じている割合（ビットエラー率）を推定する。その上で・・・

盗聴の程度に応じて秘密鍵を作る



エラー訂正

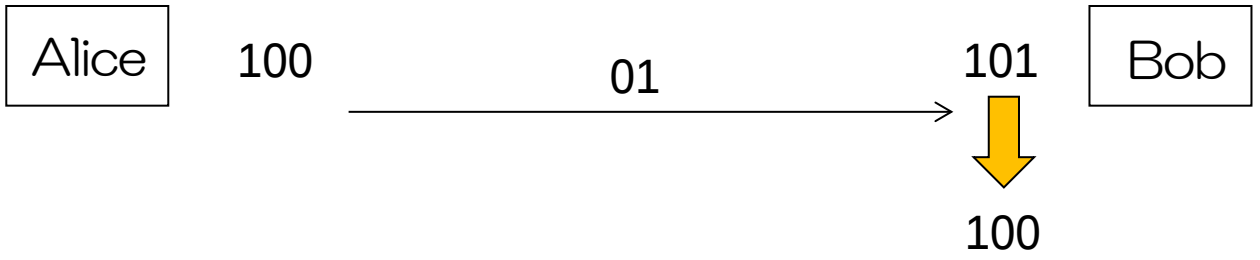
簡単な例

仮定：３ビットのうち、最大１ビットにエラー

A(00)	B(01)	C(10)	D(11)
000	100	010	001
111	011	101	110

Aliceは自分のビット列がA～Dのどれに属するかを告げる（２ビット）。

Bobは残る二つの可能性のうちで自分のビット列との食い違いが少ないほうを選ぶ。



エラー訂正

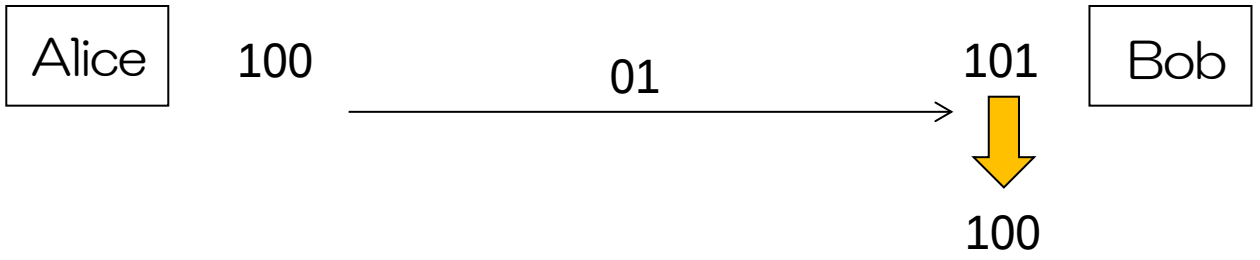
簡単な例

仮定：３ビットのうち、最大１ビットにエラー

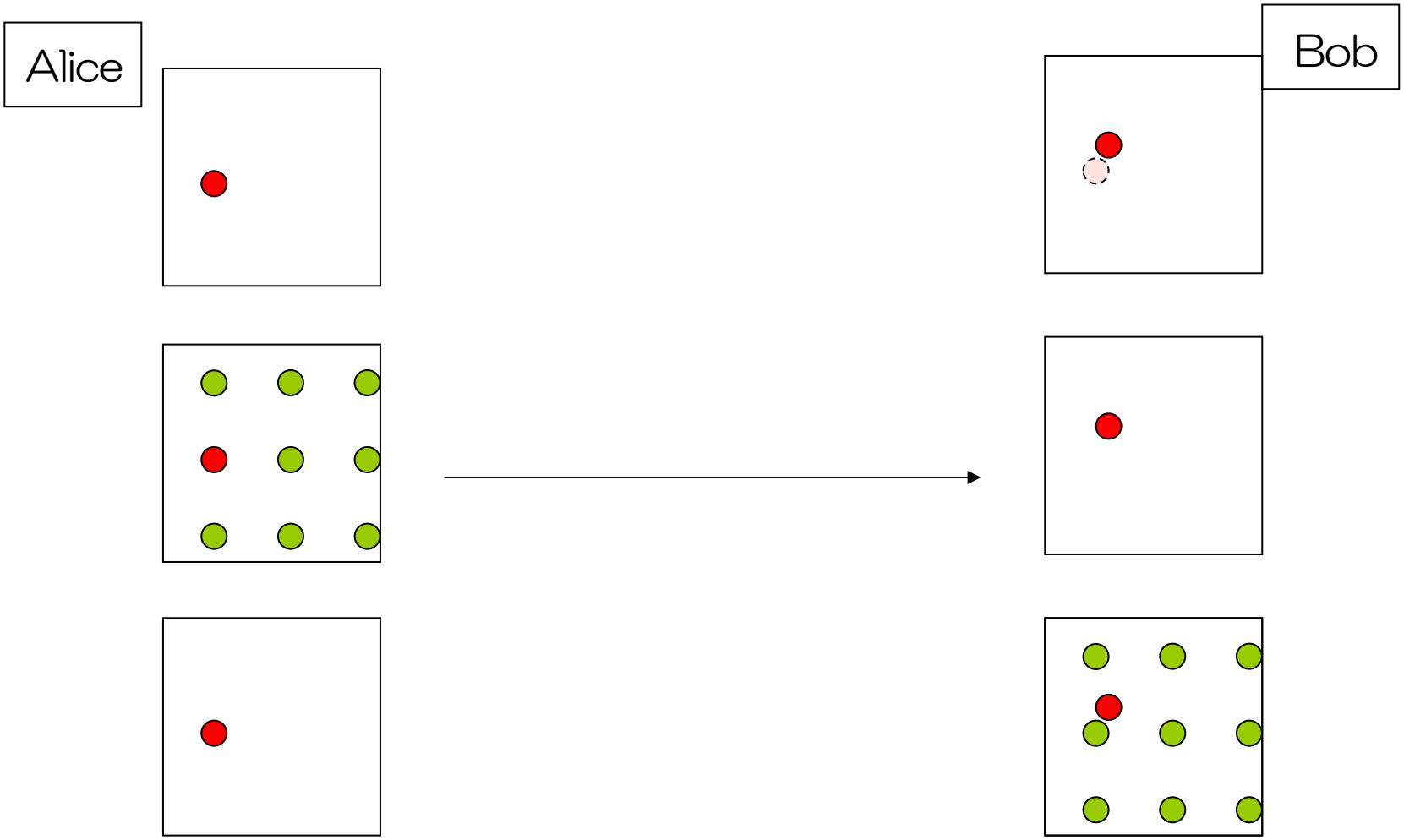
A(00)	B(01)	C(10)	D(11)
000	100	010	001
111	011	101	110

Aliceは自分のビット列がA～Dのどれに属するかを告げる（２ビット）。

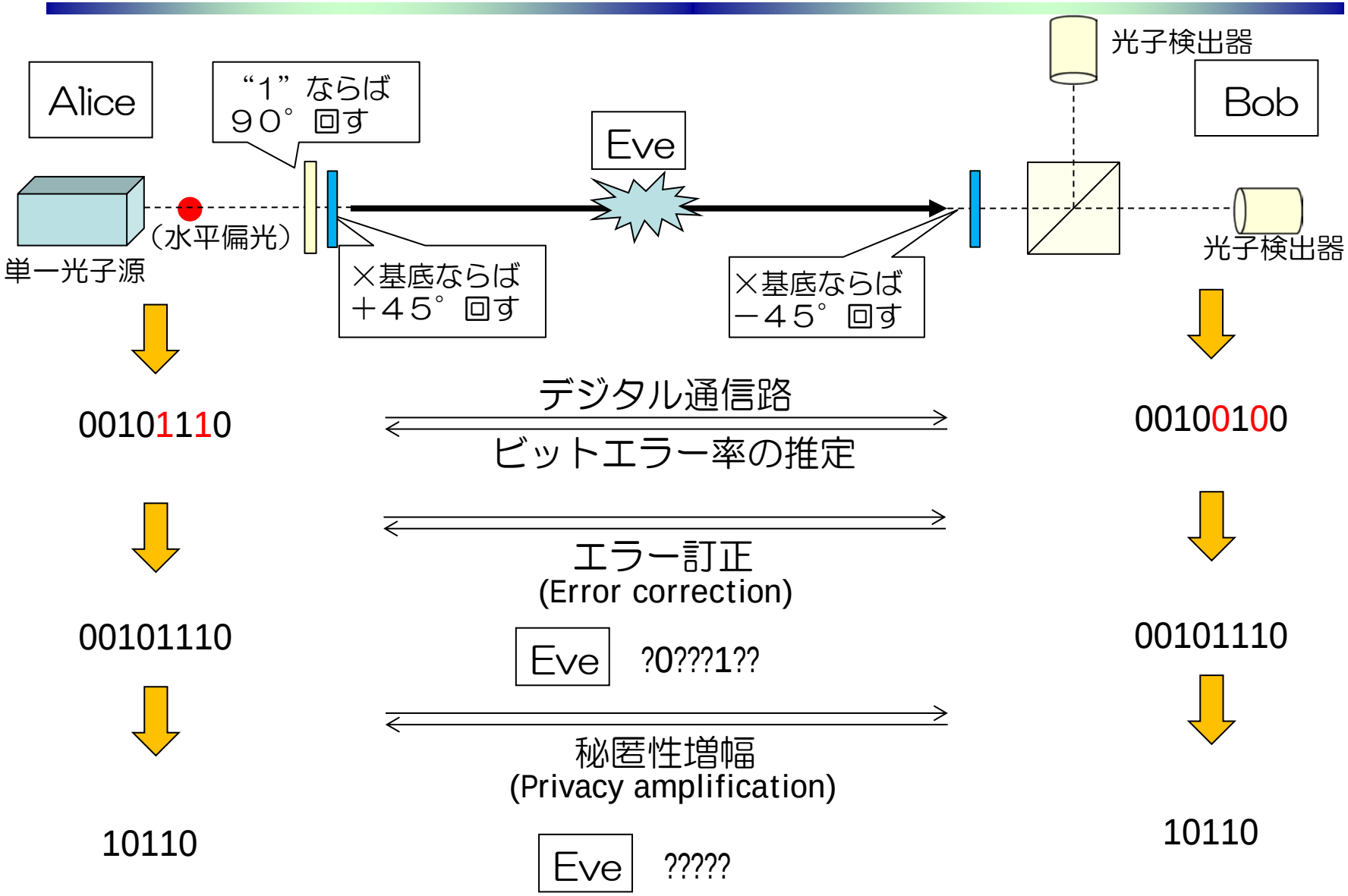
Bobは残る二つの可能性のうちで自分のビット列との食い違いが少ないほうを選ぶ。



エラー訂正



盗聴の程度に応じて秘密鍵を作る



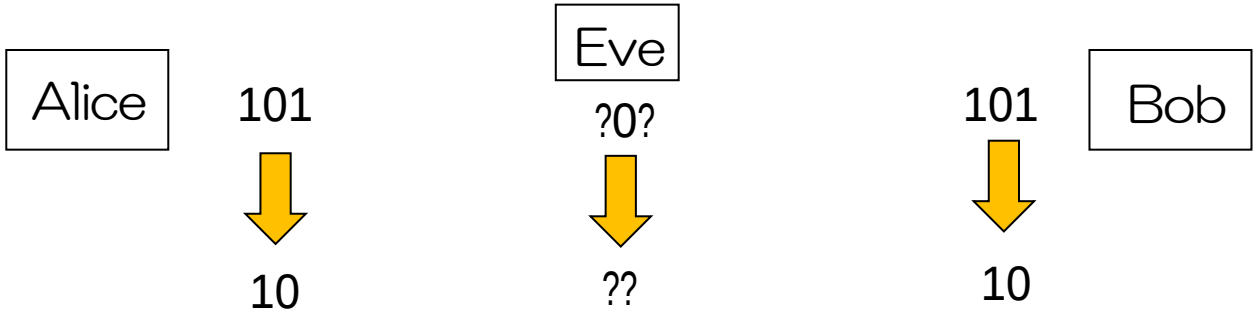
秘匿性増幅

簡単な例

仮定：３ビットのうち、Eveは最大１ビットを知っている。

A(00)	B(01)	C(10)	D(11)
000	100	010	001
111	011	101	110

AliceとBobは自分のビット列がA～Dのどれに属するかを調べ、
その答え（２ビット）を秘密鍵とする



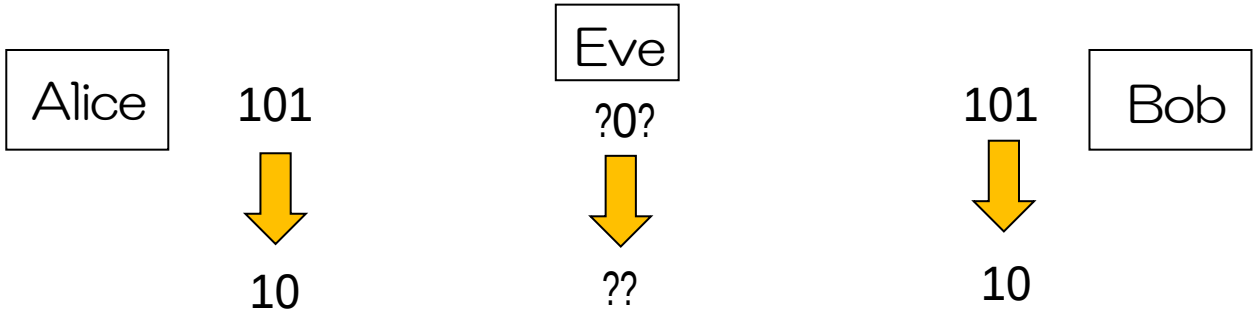
秘匿性増幅

簡単な例

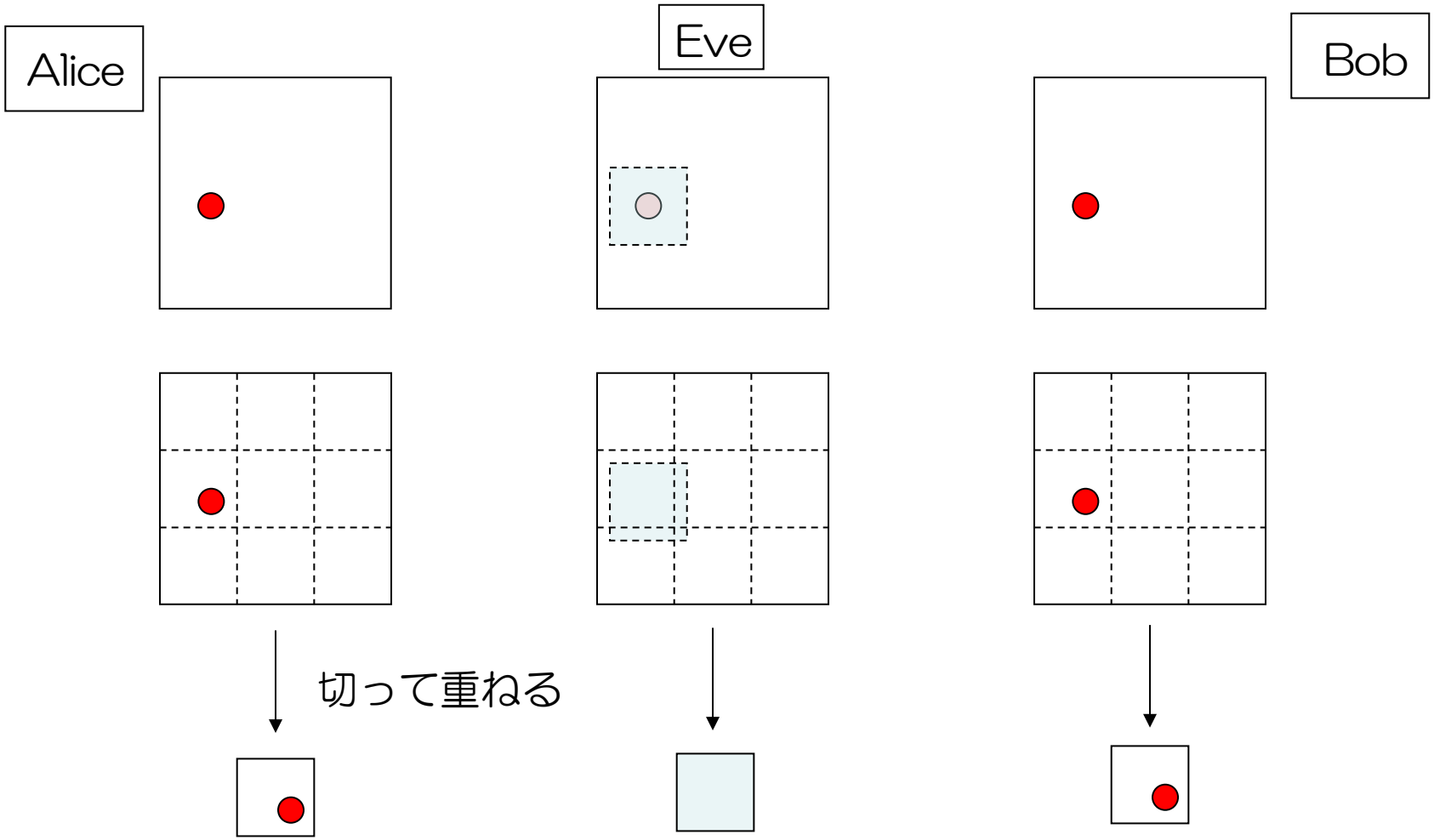
仮定：３ビットのうち、Eveは最大１ビットを知っている。

A(00)	B(01)	C(10)	D(11)
000	100	010	001
111	011	101	110

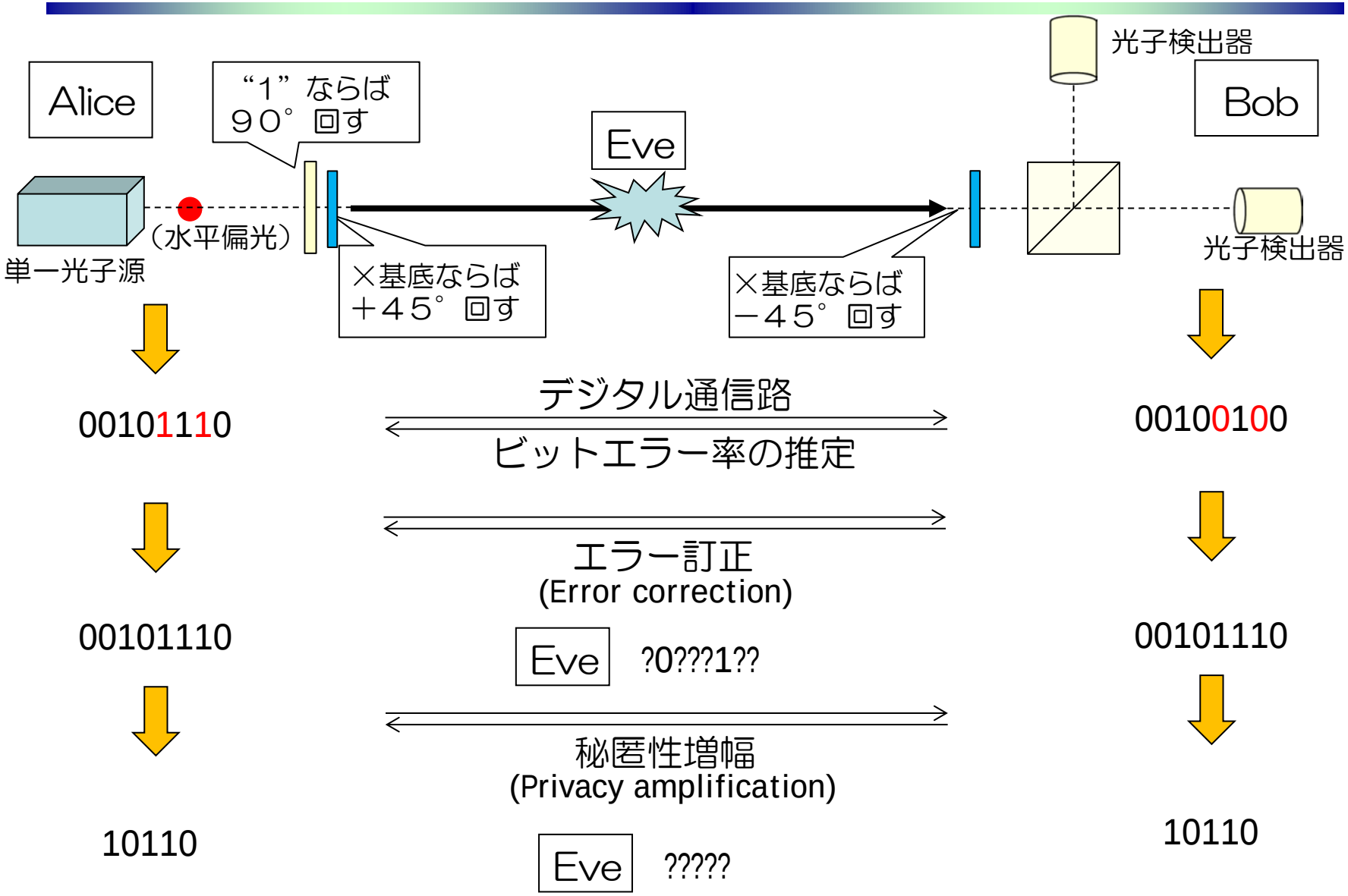
AliceとBobは自分のビット列がA～Dのどれに属するかを調べ、
その答え（２ビット）を秘密鍵とする



秘匿性増幅



盗聴の程度に応じて秘密鍵を作る



Q&A

- 単一光子源がないと出来ないの？

  レーザー光源で量子鍵配送を行う方式もある。
  また、光子検出器ではなく光検出器を用いる方式もある。

- 秘匿性増幅でビット列をどのくらい短くすればいいの？

  測定したビットエラー率から、例えば、
  「ＸＸ%まで短くすれば、秘密鍵が少しでも漏えいしている
  確率は 10^{-8} 以下」
  などの保証をセキュリティ理論から導ける。

  方式によっては理論が未完成のものもある。

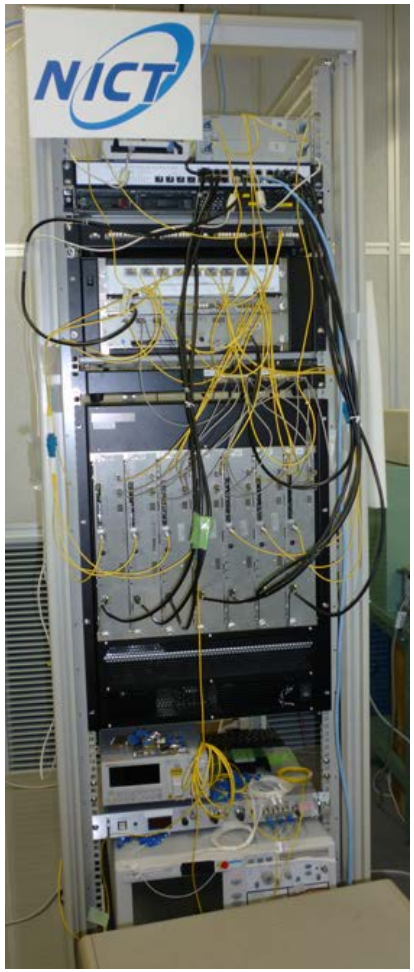
- セキュリティの前提として何を仮定しているの？

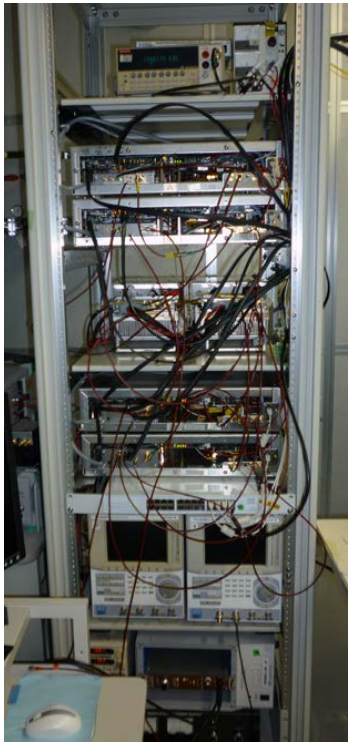
  量子力学が正しい限り、盗聴者が何をしても大丈夫。
  ただし、送受信者の装置は、理論通りに動いている必要がある。

量子暗号装置の例

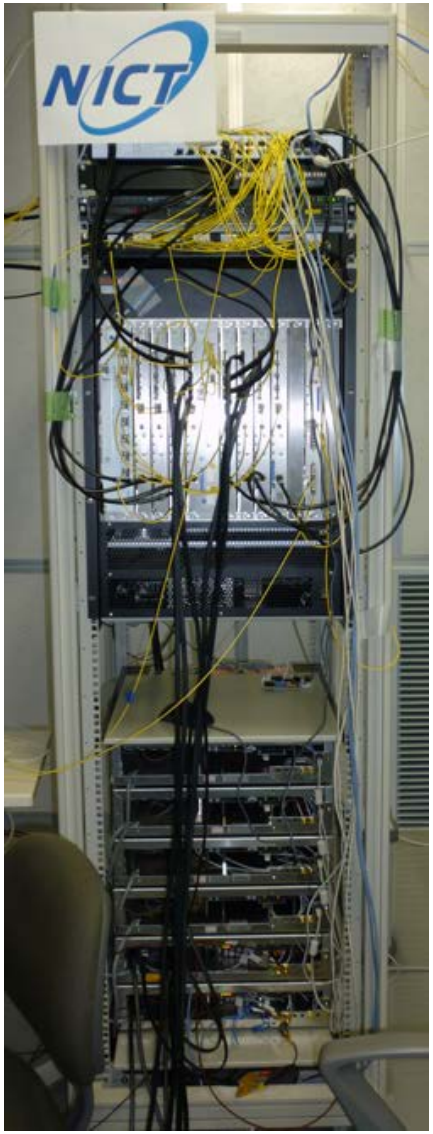
送信機

受信機

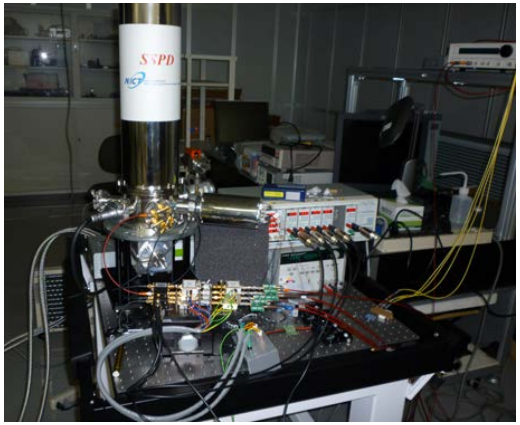




半導体光子検出器



秘密鍵蒸留装置



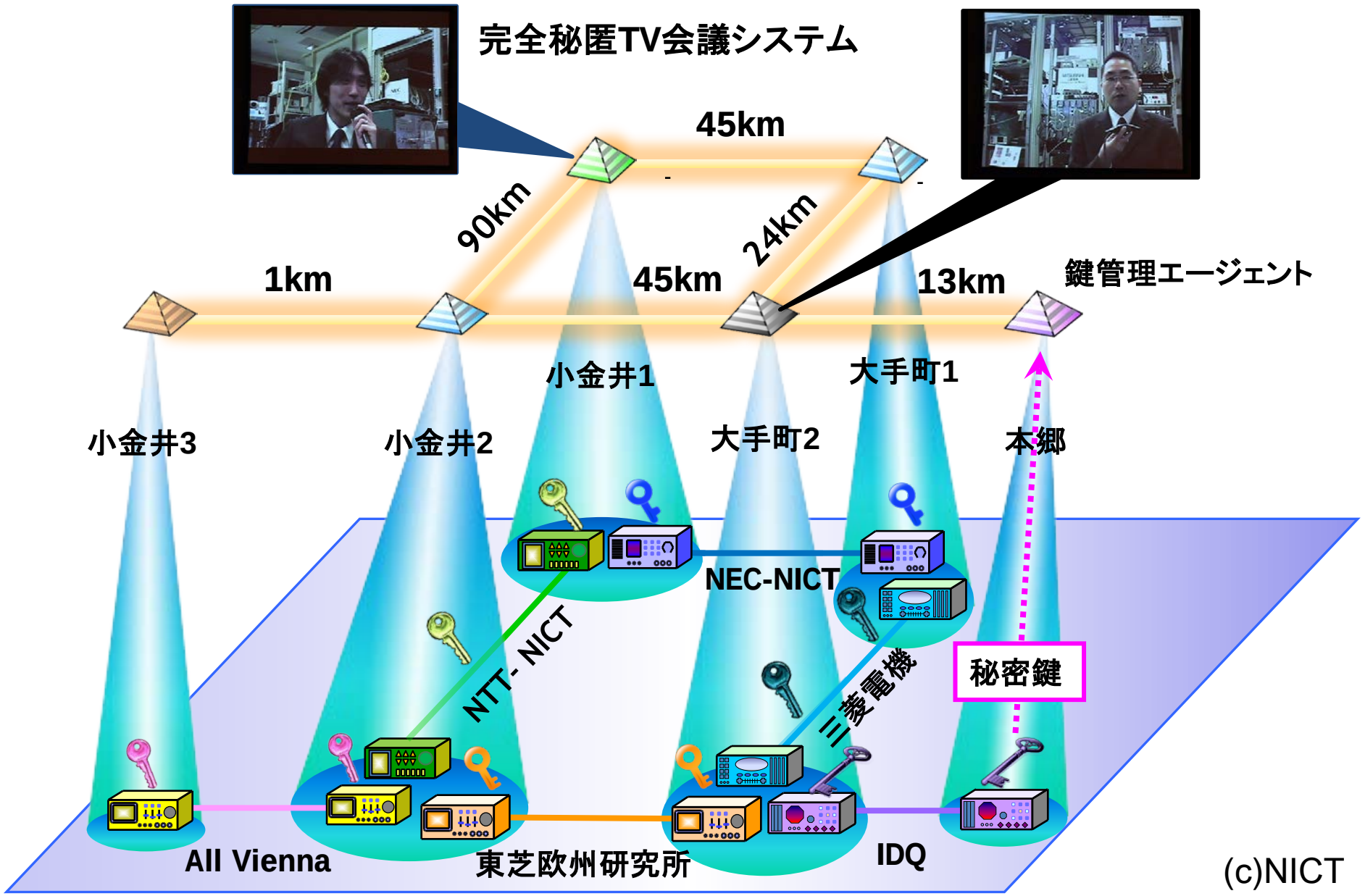
超伝導光子検出器

ＮＥＣとＮＩＣＴの共同開発

Tokyo QKD Network

＊ 地図出典：白地図専門店
http://freemap.jp/

Tokyo QKD Network



もっと遠くへ

光ファイバの透過率：最大で、～ 0.2 dB/km

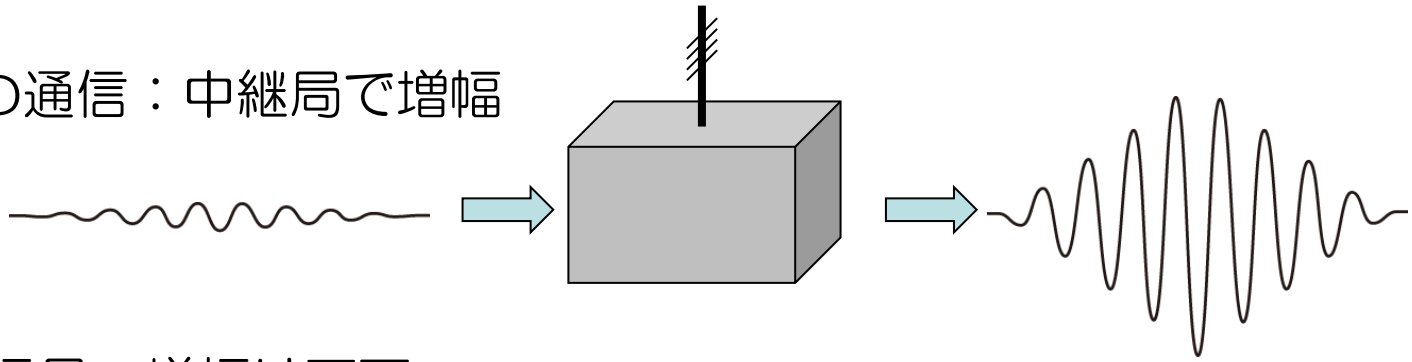
50 km で、1/10

100 km で、1/100

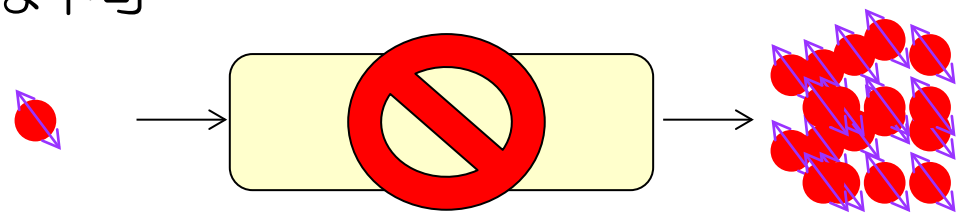
500 km で、1/10000000000

光ファイバでの直接伝送では、100~200 kmが限界

通常の通信：中継局で増幅



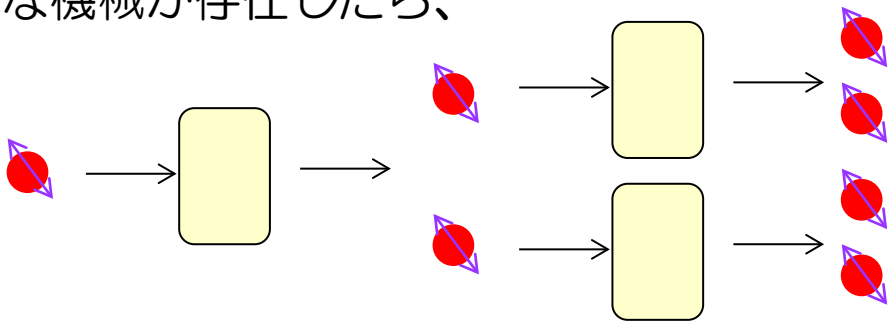
量子信号：増幅は不可



量子力学における禁止事項

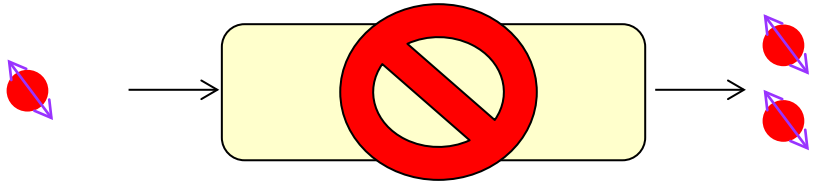
いろいろな量子状態の複製を作る機械は存在しない（No-cloning 定理）。

そんな機械が存在したら、



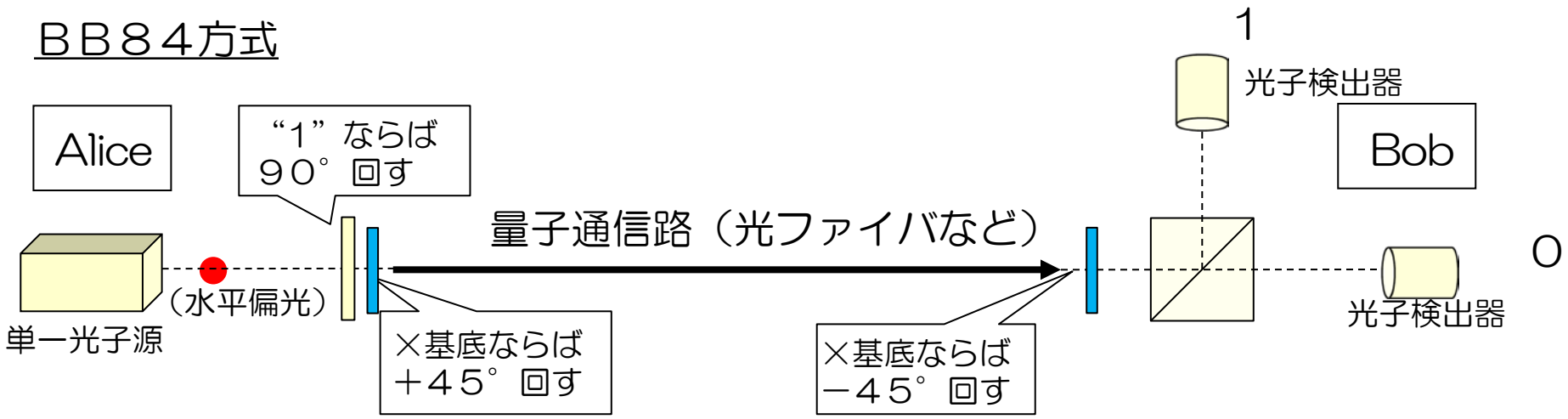
同じ偏光を持つ光子を無数に作れる。
すると、偏光方向が良い精度で決定出来てしまう。

任意の偏光の１光子をもらい、同じ偏光を持つ光子のコピーを作る機械は存在しない



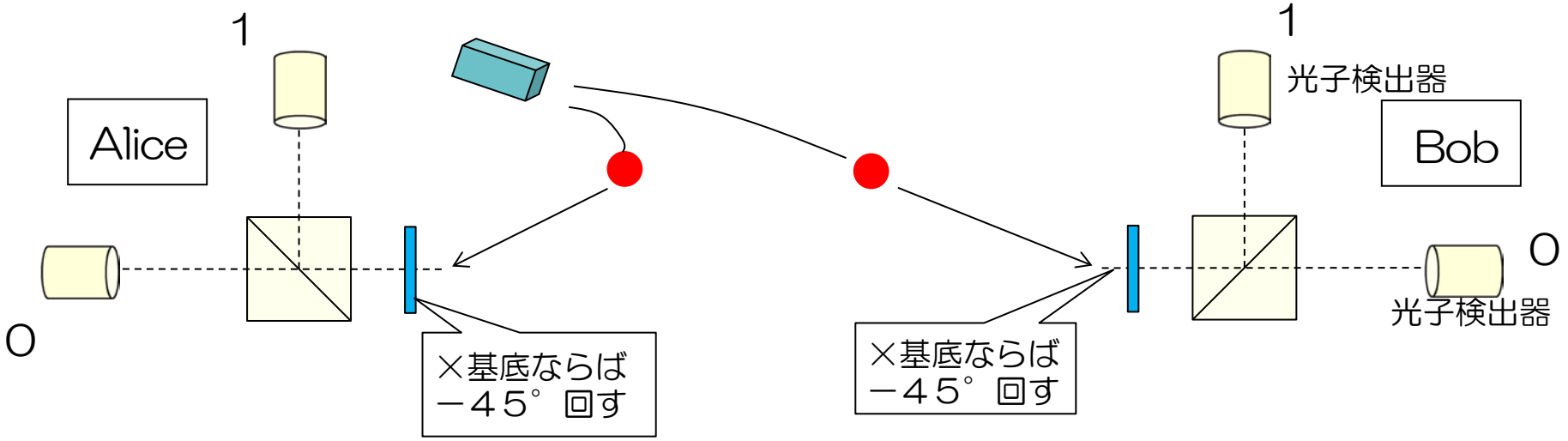
双子の光子対を用いた量子暗号

ＢＢ８４方式

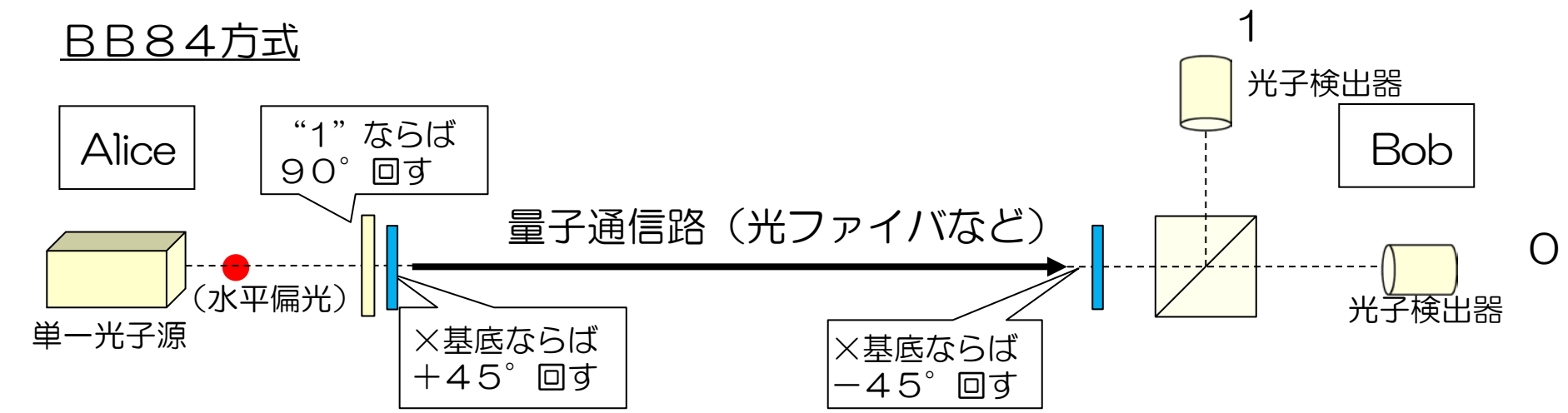


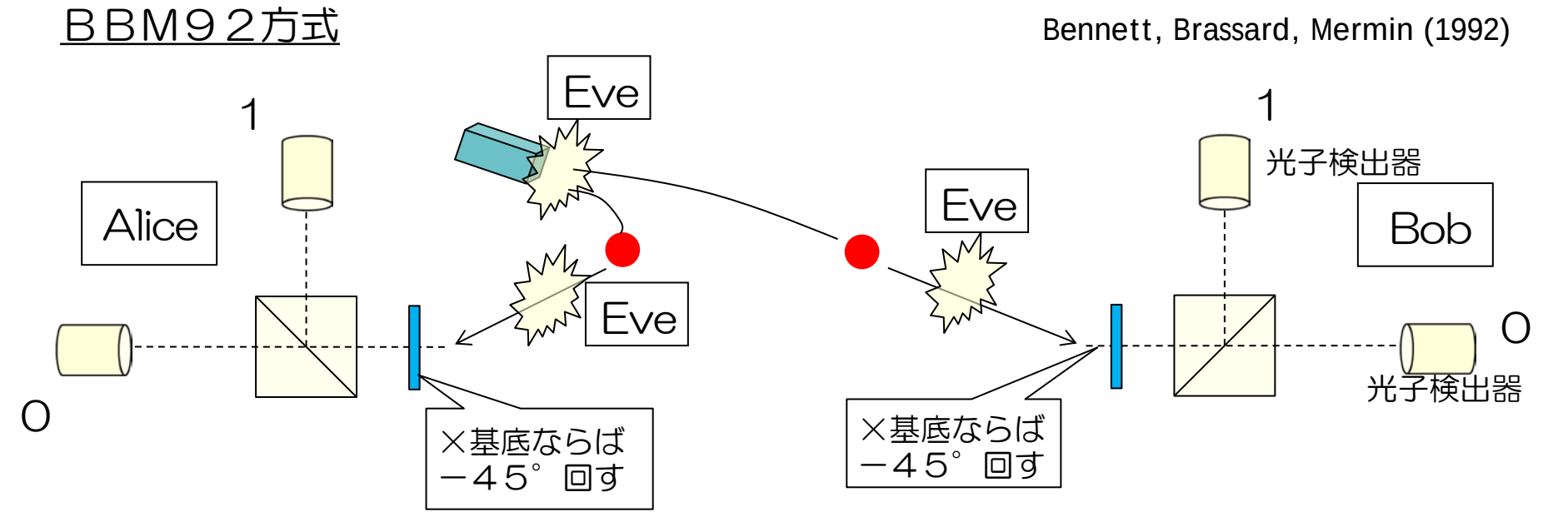
ＢＢＭ９２方式

Bennett, Brassard, Mermin (1992)



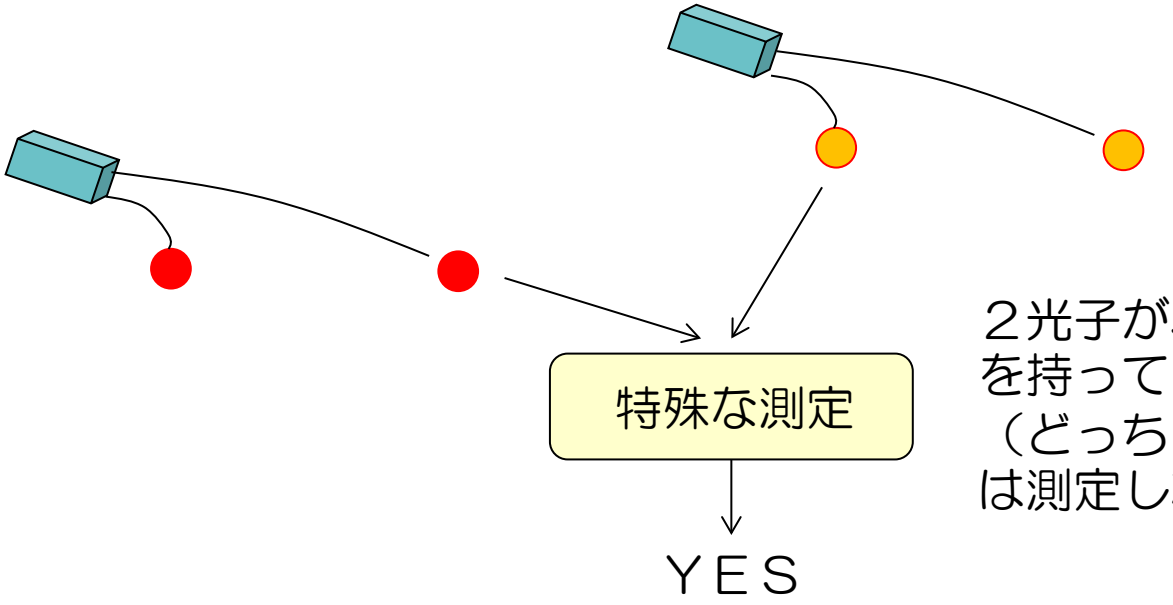
双子の光子対を用いた量子暗号



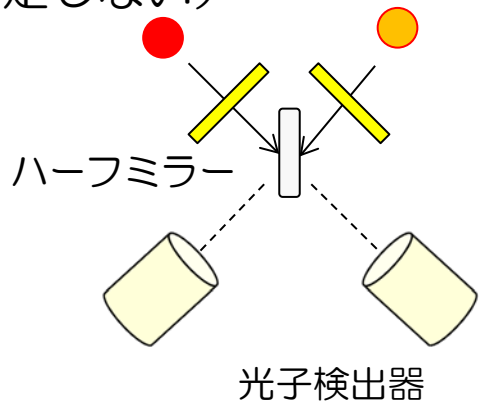


双子の光子対をつなげる

双子の光子対の性質：常に同じ偏光方向を持つ

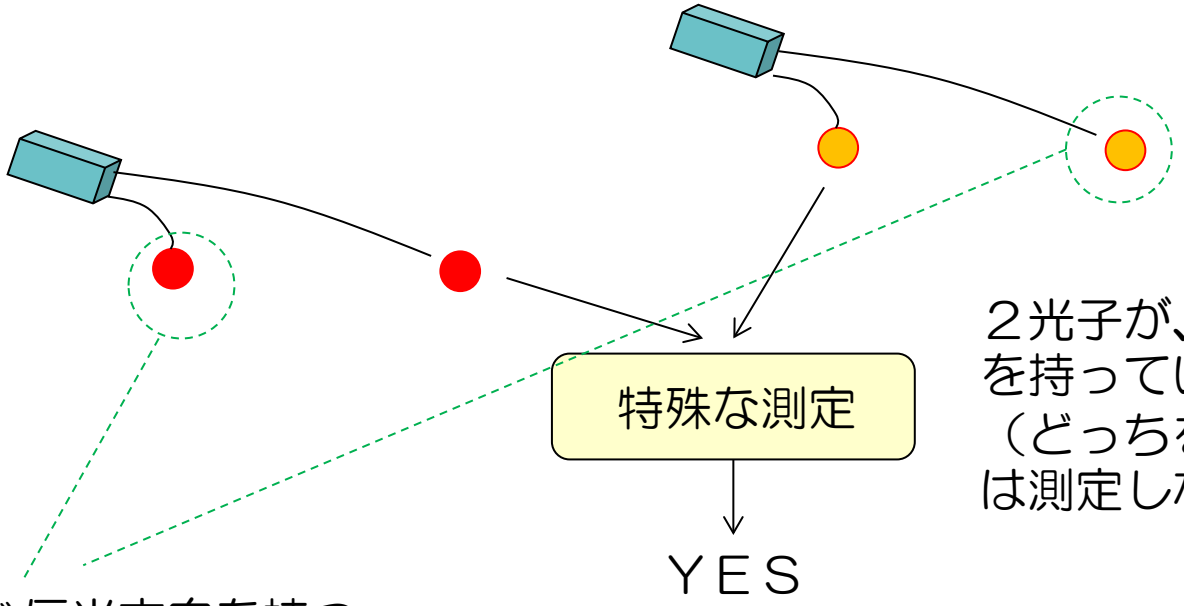


２光子が、同じ偏光方向を持っているか？
（どっちを向いているかは測定しない）



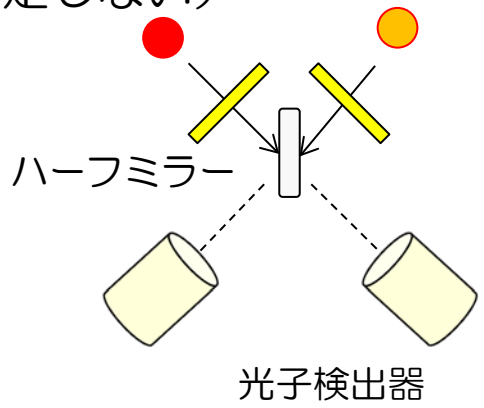
双子の光子対をつなげる

双子の光子対の性質：常に同じ偏光方向を持つ



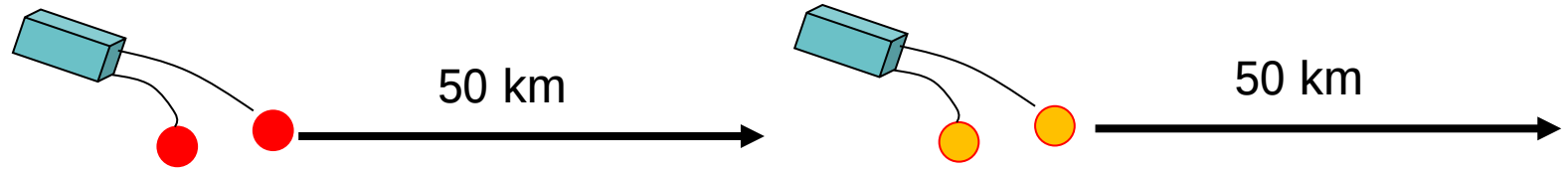
常に同じ偏光方向を持つ
＝双子の光子対になる。

２光子が、同じ偏光方向を持っているか？
（どっちを向いているかは測定しない）

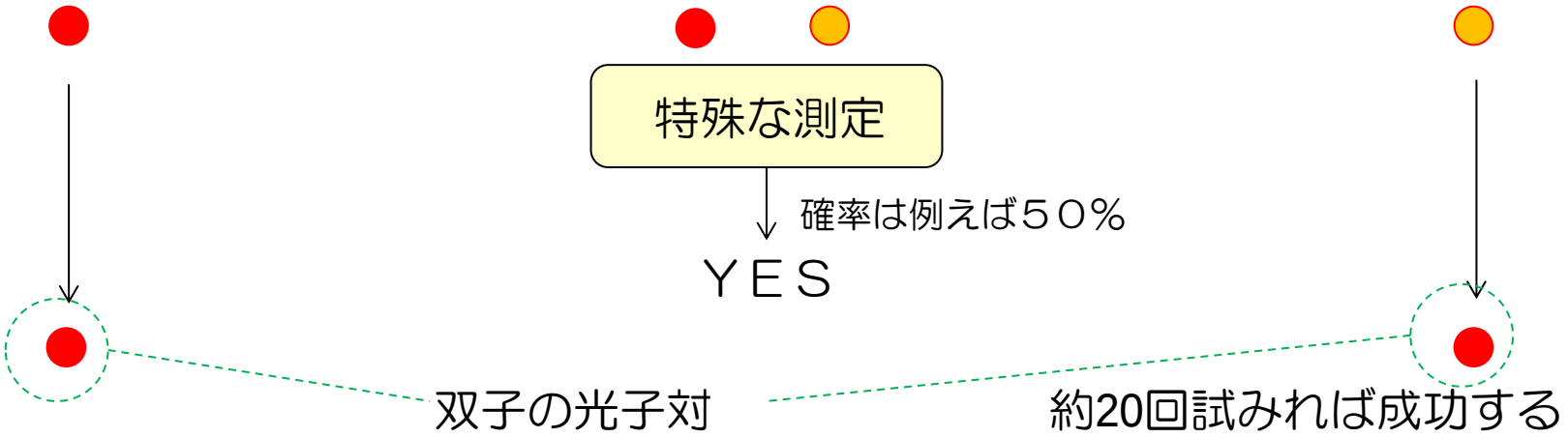


Entanglement swapping
Teleportation of entanglement

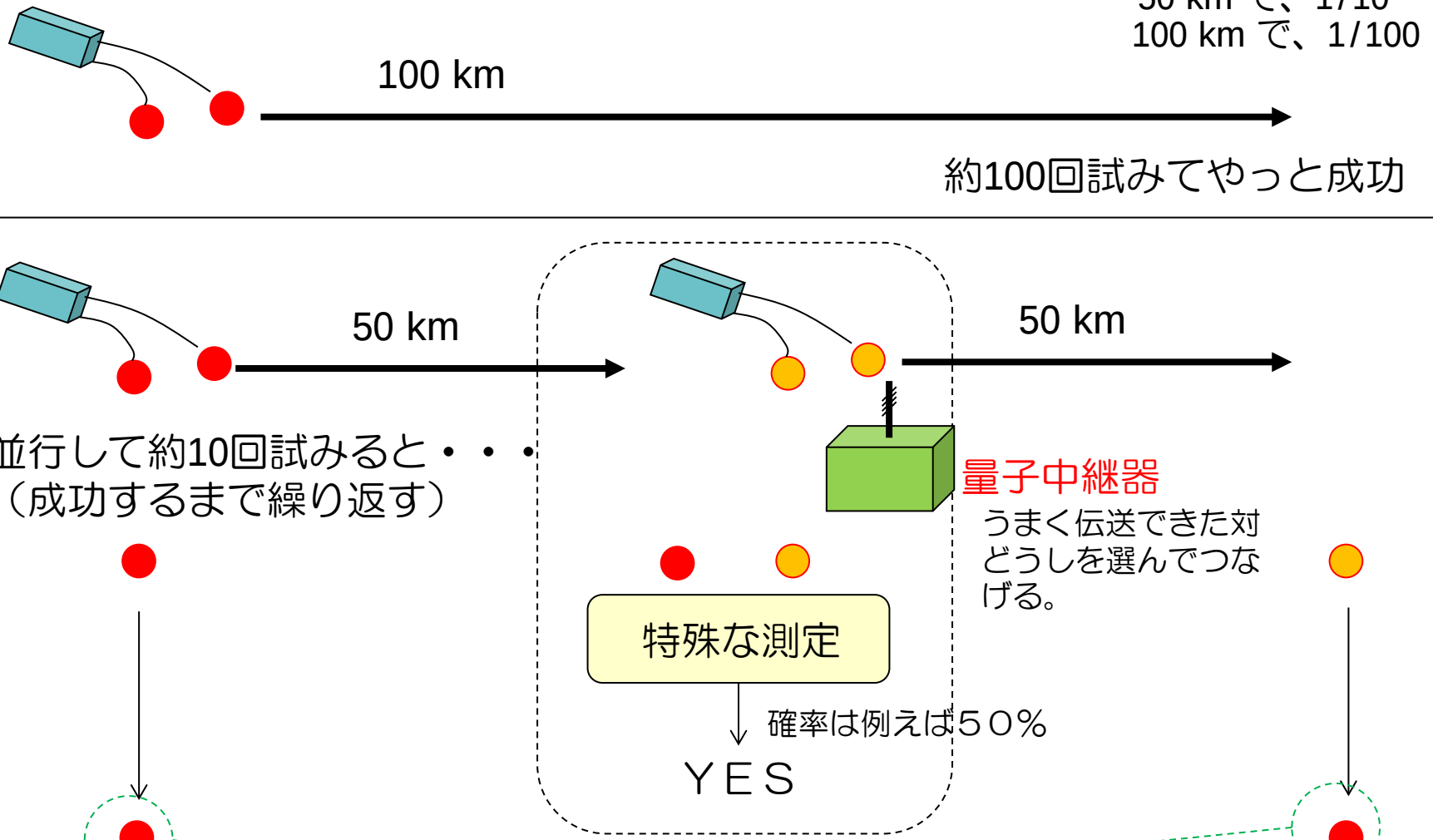
量子中継



並行して約10回試みると・・・
（成功するまで繰り返す）

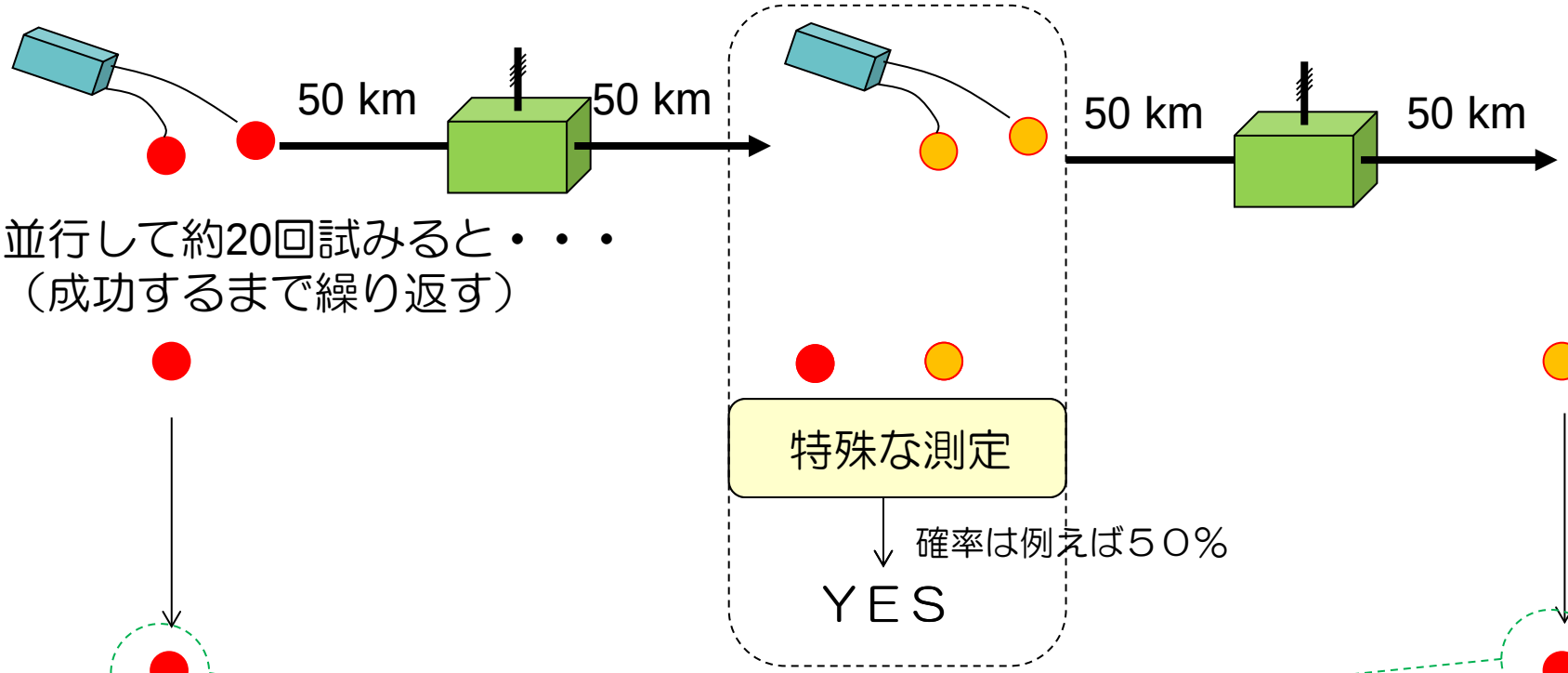


量子中継


50 km で、1/10
100 km で、1/100
100 km
約100回試みてやっと成功
50 km
50 km
並行して約10回試みると・・・
（成功するまで繰り返す）
量子中継器
うまく伝送できた対どうしを選んでつなげる。
特殊な測定
確率は例えば５０％
ＹＥＳ
双子の光子対
約20回試みれば成功する

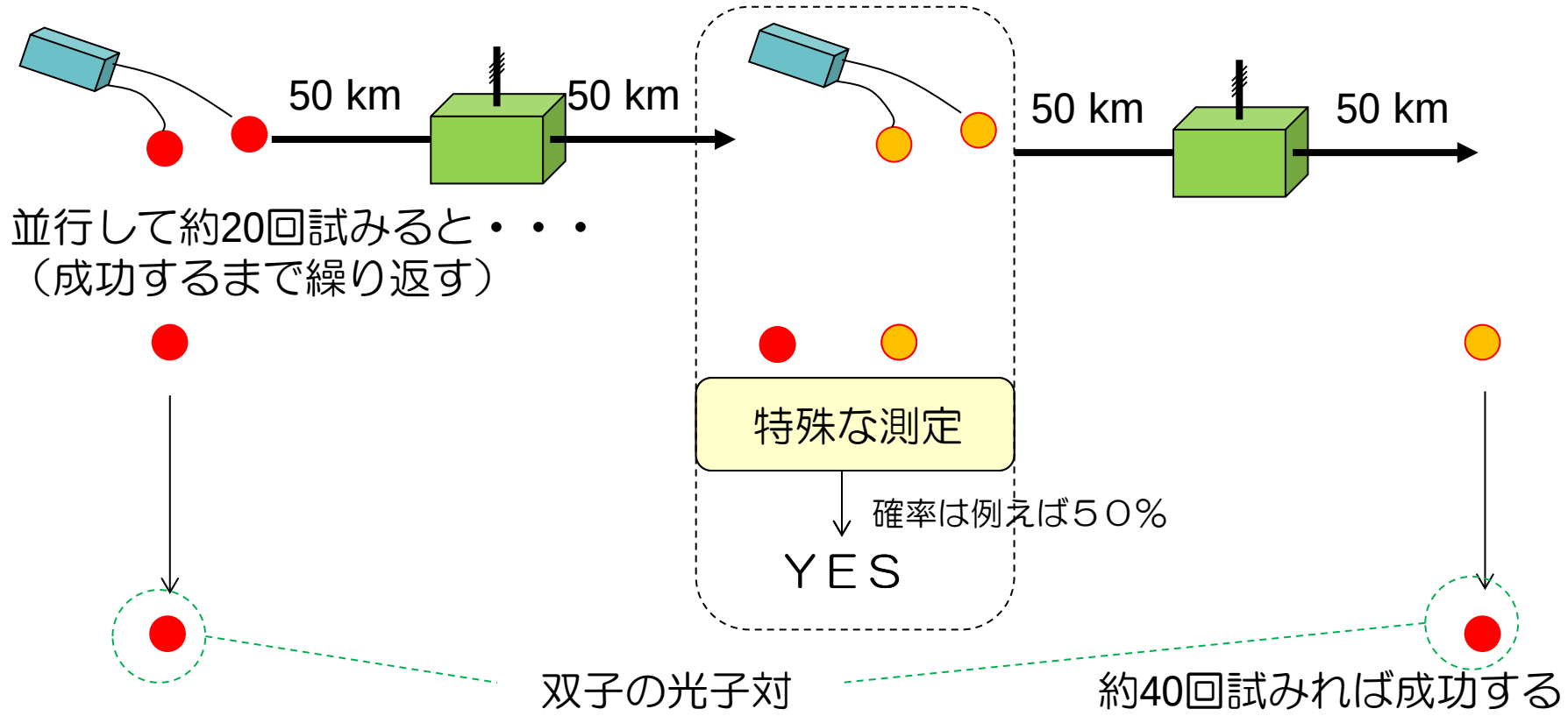
量子中継

約10000回試みてやっと成功



量子中継

- 光子の到着を、光子を破壊せずに検知する技術
- 光子の偏光方向（量子状態）を物質にそのまま移しかえる技術
- 物質の量子状態を壊さず保持する技術（量子メモリ）
- 物質から光に量子状態を戻す技術
- 物質のままで特殊な測定を行う技術

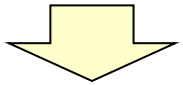


量子力学を超えて

Post-quantum-world cryptography

量子暗号：量子力学が正しいことを前提に、セキュリティを保証

量子力学ではなぜ測定が制限されるか、という理由のひとつは、
「なんでもかんでも測定できちゃうと超光速通信になるから」



「もし盗聴出来てしまったら、必ず超光速通信ができてしまう」
というような議論でセキュリティを保証できないだろうか？

（量子力学は議論に登場しない）

メリット：

- 量子力学が将来修正されることになっても、セキュリティは揺るがない。
- 送受信者の装置の中身がどうなっているかは、気にしなくてよい。

Q&A

- 単一光子源がないと出来ないの？

  レーザー光源で量子鍵配送を行う方式もある。
  また、光子検出器ではなく光検出器を用いる方式もある。

- 秘匿性増幅でビット列をどのくらい短くすればいいの？

  測定したビットエラー率から、例えば、
  「ＸＸ%まで短くすれば、秘密鍵が少しでも漏えいしている
  確率は 10^{-8} 以下」
  などの保証をセキュリティ理論から導ける。

  方式によっては理論が未完成のものもある。

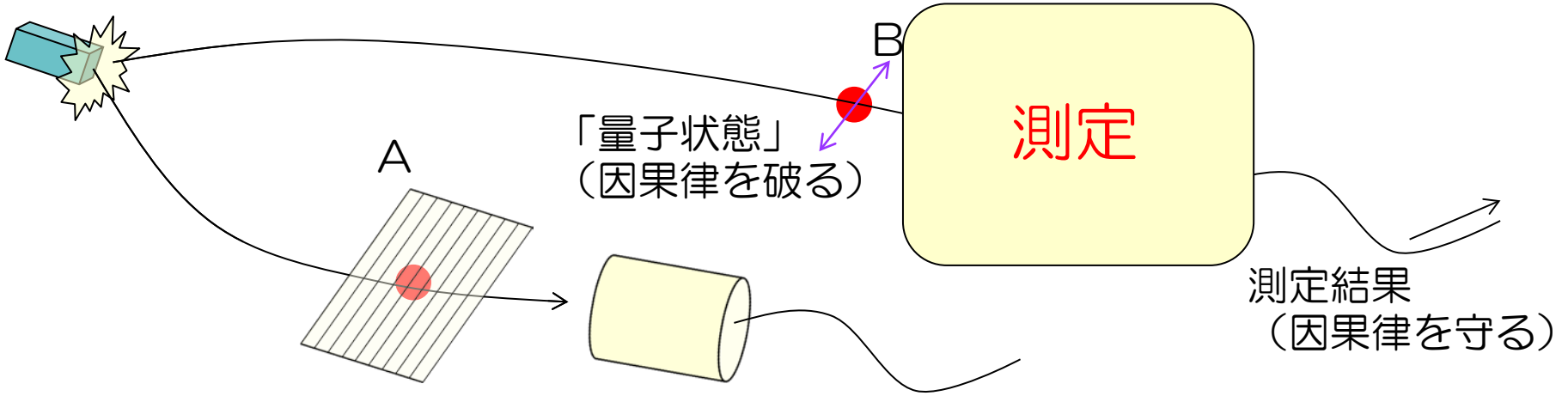
- セキュリティの前提として何を仮定しているの？

  量子力学が正しい限り、盗聴者が何をしても大丈夫。
  ただし、送受信者の装置は、理論通りに動いている必要がある。

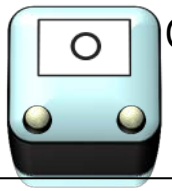
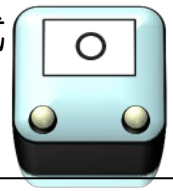
量子力学を超えて

何故我々の住む宇宙は量子力学なのか？？

量子力学と因果律

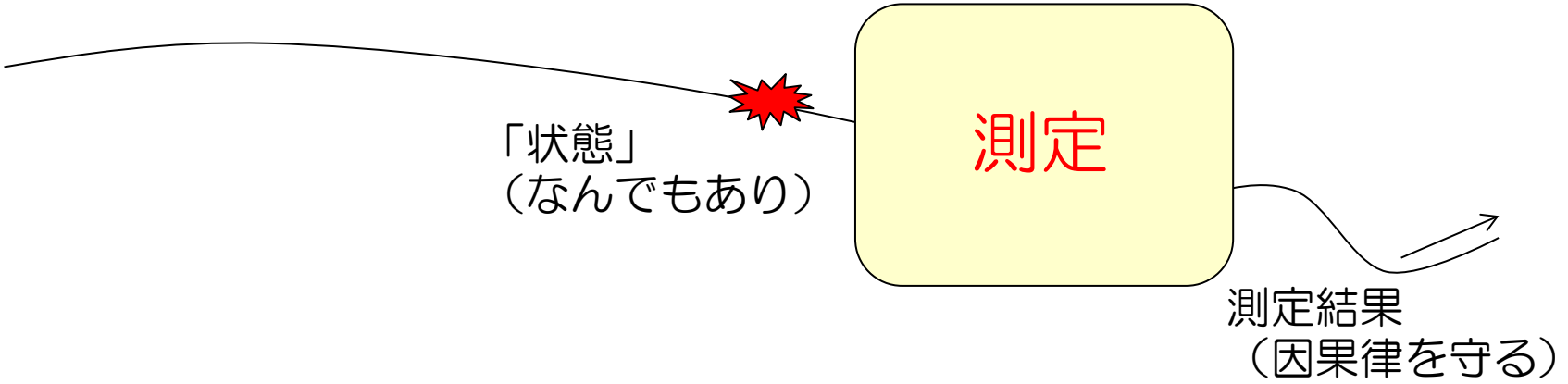


これまでは、測定前の「状態」が、因果律を破るように見えて気持ちが悪い、という話であった。

	 当たりの確率 P 	 CHSH不等式 S 
測定前の「状態」も因果律を守るなら・・	$P \geq 1/3$	$S \leq 2$
量子力学	$P \geq 1/4$	$S \leq 2\sqrt{2}$

ちなみに、量子力学では、これらの数字を超えることは不可能だということが証明されている。

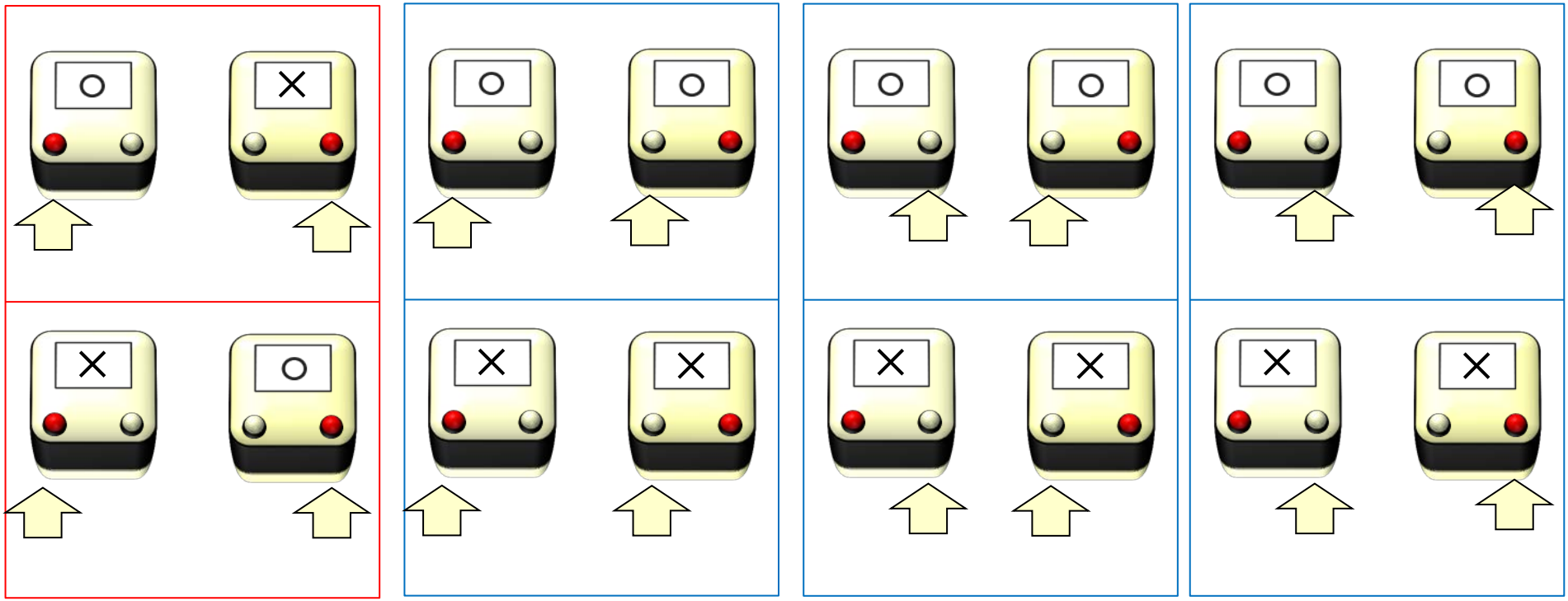
量子力学を超えて



逆に、開き直って、目に見える結果さえ因果律を守っていれば、後ろのからくりは何でもあり、という世界を想像してみよう。すると・・

量子力学を超えて

こんな機械があっても良いことになる。

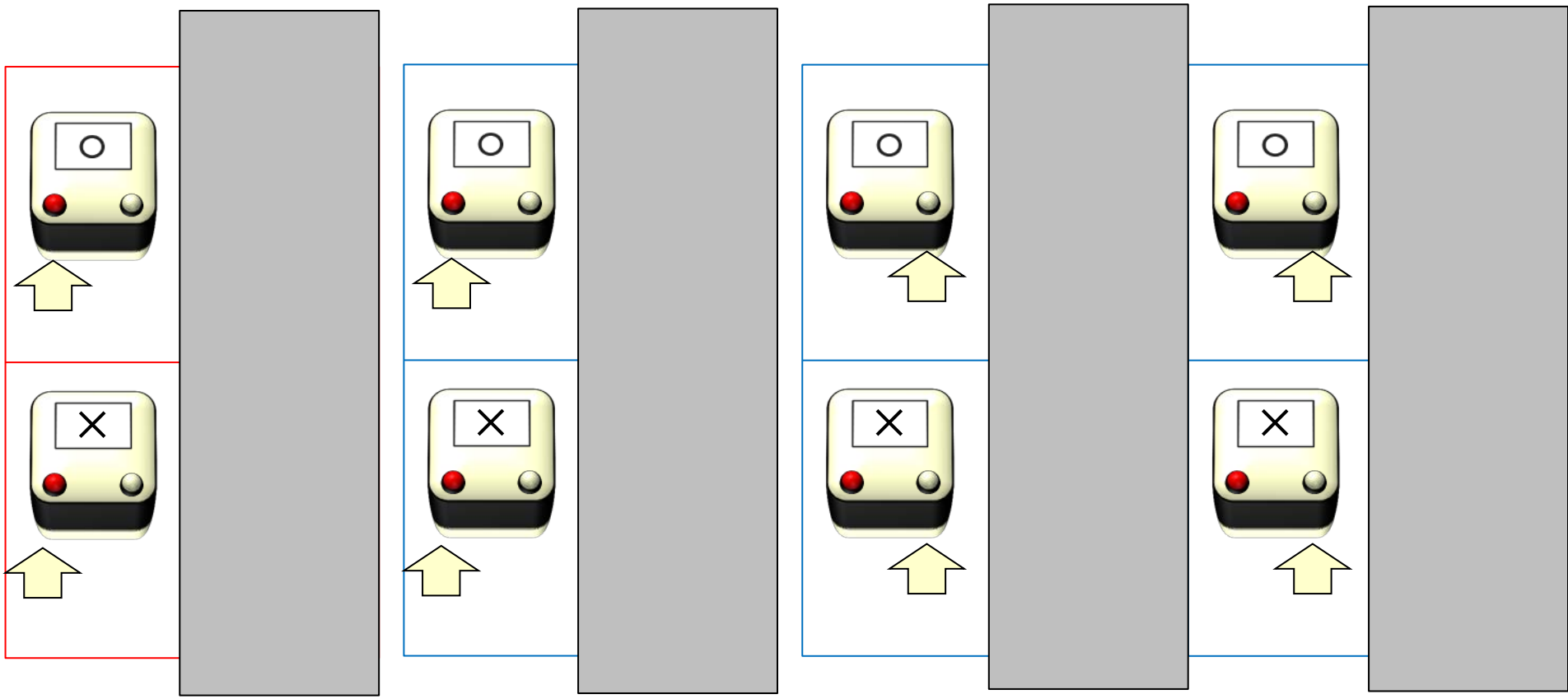


両方とも赤ボタンが押されたときだけ、違うマークが出る。

Popescu & Rohrlich (1994)

量子力学を超えて

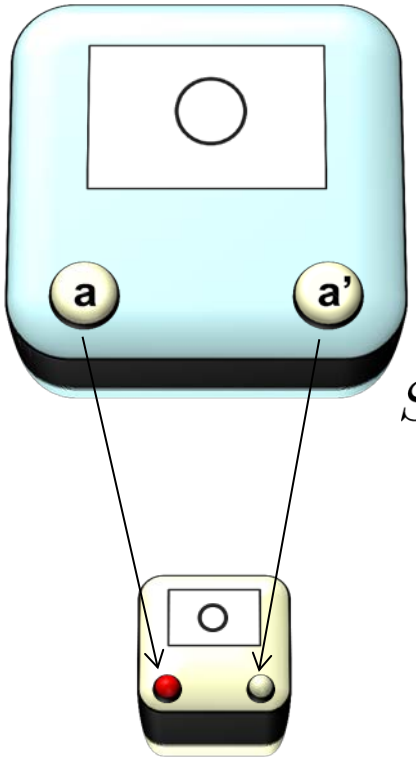
こんな機械があっても良いことになる。



片側だけの機械を見ると、どんな場合でも○×がランダムに出るだけなので、もう一方の機械のどちらのボタンが押されたかはわからない。
（超光速通信にはならない）

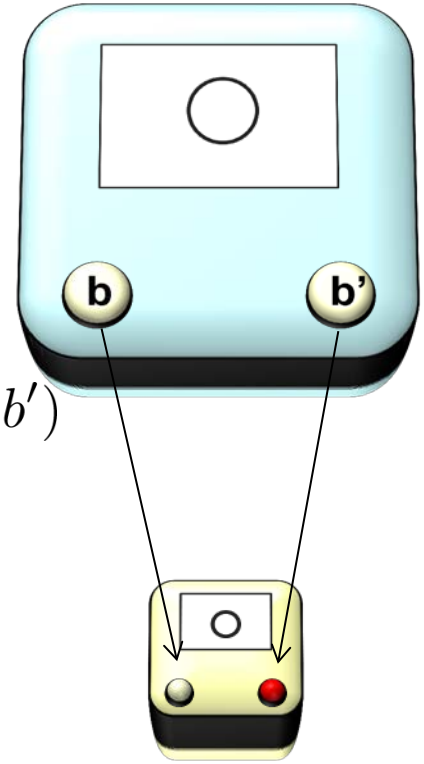
Popescu & Rohrlich (1994)

CHSHの場合



同じマークなら１点、
違うマークなら（－１）点とする。

aとbのボタンが押された場合の平均点
（期待値）を $E(a,b)$ と書く。

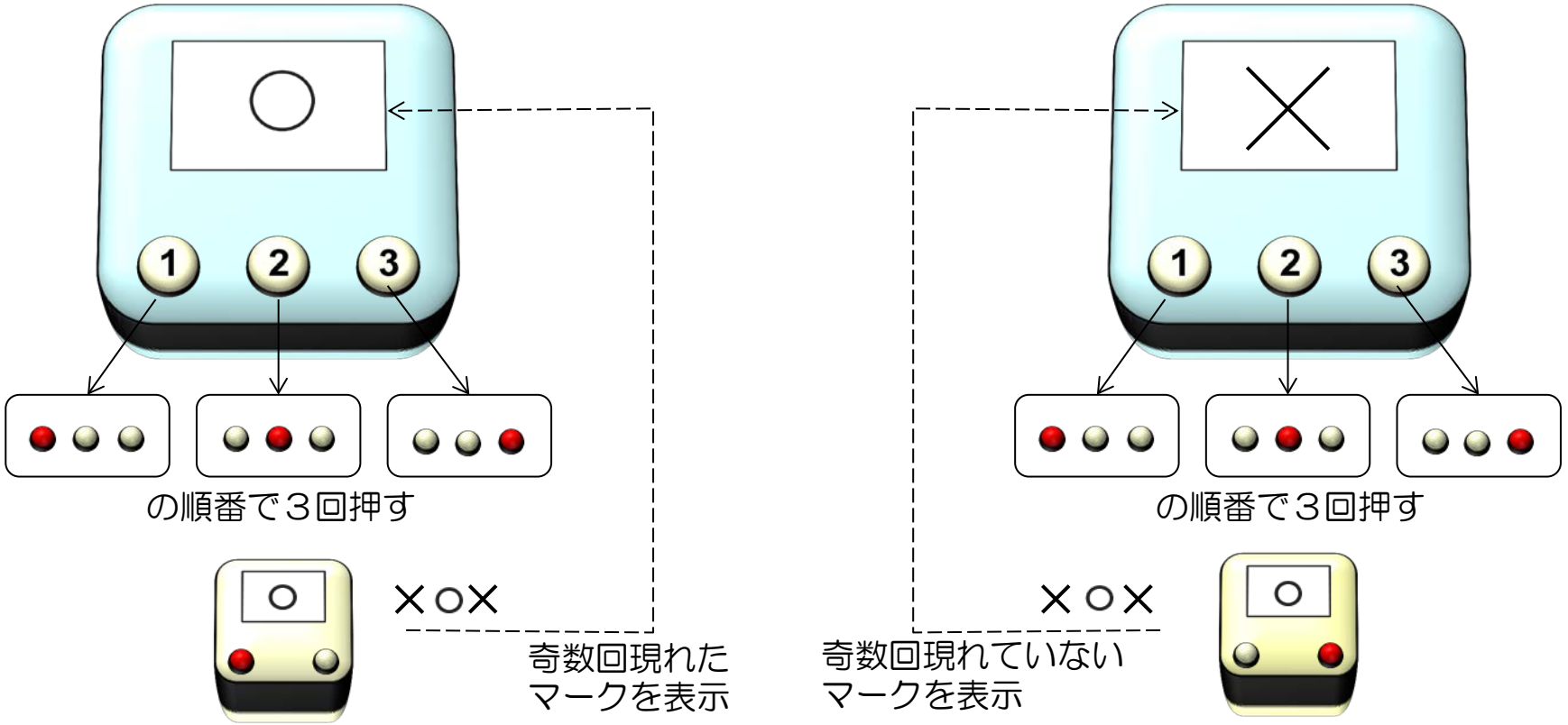


$$S \equiv E(a,b) - E(a,b') + E(a',b) + E(a',b')$$

$$S = 1 - (-1) + 1 + 1 = 4$$

３ボタンゲームの場合

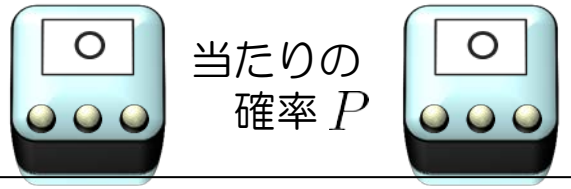
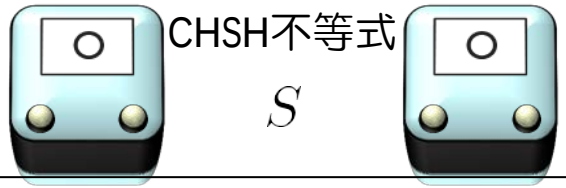
同じ番号のボタンが押されたら、〇か×か必ず同じマークがでる。
違う番号のボタンを押して、マークが一致したら当たり。



当たりの確率はゼロ！

量子力学を超えて

何故我々の住む宇宙は量子力学なのか？？

	 当たりの確率 P	 CHSH不等式 S
測定前の「状態」も因果律を守るなら・・	$P \geq 1/3$	$S \leq 2$
量子力学	$P \geq 1/4$	$S \leq 2\sqrt{2}$
測定結果さえ因果律を守るなら、あとは何でもありの世界	$P \geq 0$	$S \leq 4$

どうせ一線を踏み越えてしまったのなら、どうして中途半端なところに踏みとどまっているのか？

この数字に特別の意味があるのだろうか？

微(かす)かな光の不思議な世界

- 第10回 12/20　光の正体と量子論の不思議
- 第11回　1/10　微弱光を用いた究極の暗号

工学系研究科　　光量子科学研究センター
物理工学専攻

小芦　雅斗