量子情報と通信技術

--「量子インターネット」という未来 --

はじめに

量子論・量子情報理論のIT技術への応用というと、多くの人は、「量子コンピュータ」のことを思い浮かべるだろう。

ただ、量子論・量子情報理論のIT技術への応用は、「量子コンピュータ」だけではないことに留意する必要がある。

小論がテーマとして取り上げる「量子情報通信」は、そのもう一つの重要な応用分野である。

僕は、「量子コンピュータ」より、「量子情報通信」の世界の「実用化」が早いのではと考えている。

はじめに

量子論・量子情報理論のIT技術への応用に対するIT技術者の関心は、数年前と比べると確実に広がっているように見える。それは歓迎すべきことだと思う。

同時に、いくつかの「誤解」も広がっているように、僕は感じている。一つ例をあげよう。

「量子コンピュータを理解するために、
量子力学を学ぶ必要がある」

それは、ほとんど誤解に近いものだと僕は思う。

はじめに

「量子情報理論」と「量子力学」とは、別のものである。

それは、「情報理論」と「力学」が、別のものであるのと同じである。

もう少し具体的に述べれば、「力学」にとって、「位置」や「運動量」や「エネルギー」は、本質的に重要な概念である。しかし、「情報理論」にとって、「位置」や「運動量」や「エネルギー」は、さしたる意味を持たない。「情報理論」で重要なのは、「エネルギー」ではなく「エントロピー」である。

はじめに

確かに、「量子力学」と「量子情報理論」は、「量子論」という共通の土台の上に成り立っている。ただ、両者の違いは大きい。

そのことは、「量子力学」の世界で、エンタングルメントが発見されてから、「量子情報理論」の世界で基本的な役割を果たす、エンタングルメントを利用する「量子テレポーテーション」が発見されるまで、60年近い年月がかかったことに、はっきりとあらわれている。

「量子情報理論」は、「量子力学」とは区別して、「量子情報理論」として学ぶ必要がある。

はじめに

小論「量子情報と通信技術」は、いわゆる「量子情報通信 Quantum Information Communication 」の世界の基本的な技術を紹介したものである。

取り上げたのは、次の四つのトピックスである。

- Quantum Key Distribution
- Quantum Teleportation
- Entanglement Swapping
- Time-Bin qubit Encoding

はじめに -- 各国・各研究グループの取り組み

はじめにの終わりに、小論では触れることのできなかった量子情報通信分野の近年（2020年-2022年）の取り組みについて、いくつかの論文のタイトルとリンクを紹介しようと思う。

次の三つの地域の研究グループの論文である。

- 中国
- アメリカ
- ヨーロッパ

それぞれのグループが、どのような「ブレークスルー」の展望をもっているのか興味のある方は、参照されたい。

はじめに -- 各国・各研究グループの取り組み
中国

2021/01/06 Nature

"An integrated space-to-ground quantum communication network over 4,600 kilometres"

https://www.nature.com/articles/s41586-020-03093-8

衛星と地上の光ファイバーをむすんだ、全長 4,600km, ノード数 109 の世界最大の量子情報ネットワーク。ユーザー数 157で、ユーザー間で、708個の量子キー配布QKDのリンクを実現。

さまざまなQKDの方式、さまざまなネットワーク・トポロジーに挑戦している。

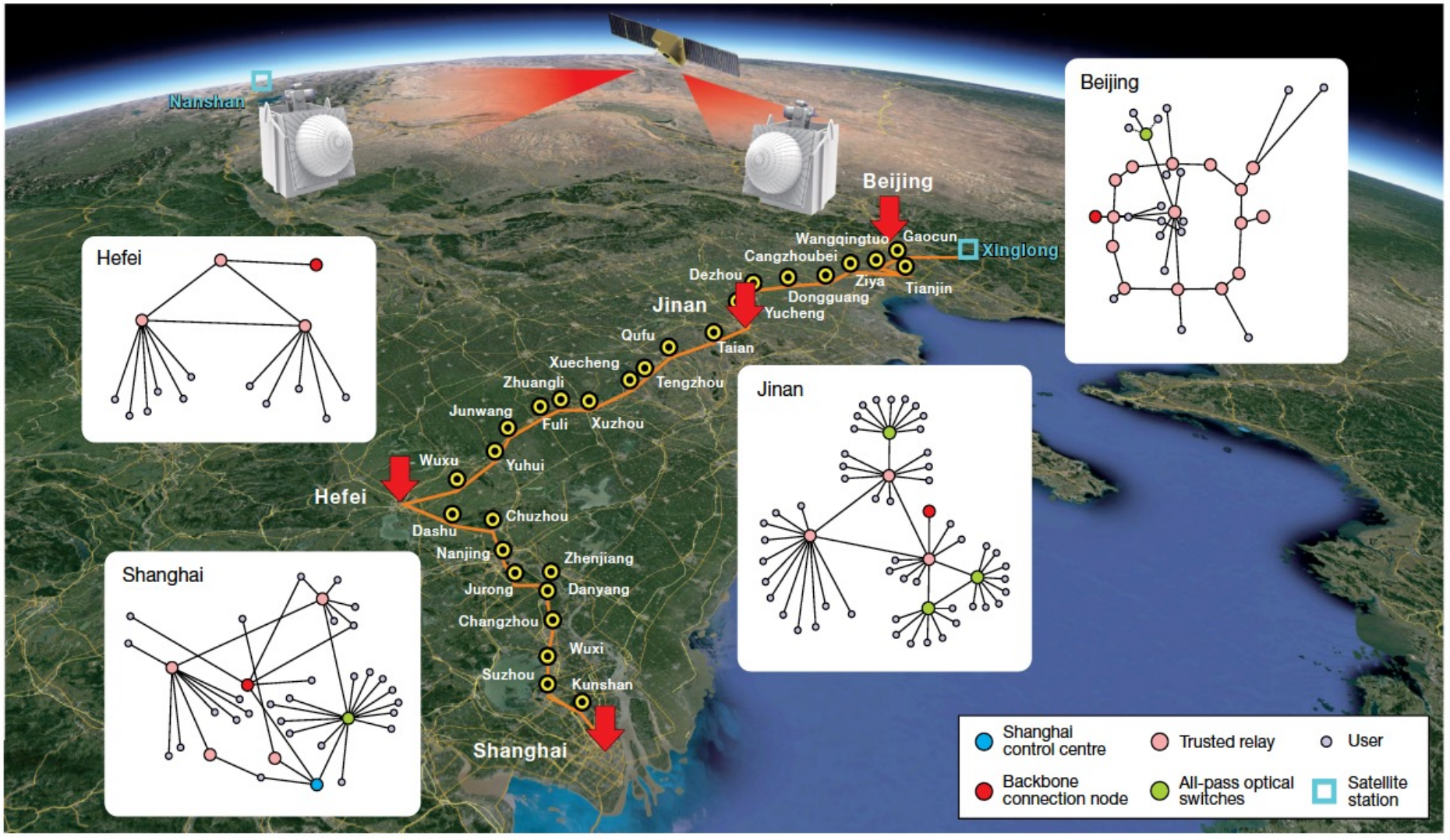


Fig. 1 | Illustration of the integrated space-to-ground quantum network. The network consists of four QMANs (in Beijing, Jinan, Shanghai and Heifei; red arrows), a backbone fibre link over 2,000 km (orange line) and two ground–satellite links that connect Xinglong and Nanshan (blue squares), separated by 2,600 km. There are three types of node in the network: user nodes (purple circles), all-pass optical switches (green circles) and trusted relays (pink circles). Each QMAN consists of all three node types (see insets). The backbone is connected by trusted relays (shown as yellow and black circles in the main image and red circles in the insets). A quantum satellite is connected to the Xinglong and Nanshan ground stations; Xinglong is also connected to the Beijing QMAN via fibre. In Beijing, the Beijing control-centre node is located at the same location as the backbone connection node (indicated by the red circle). Map data: Google, Data SIO, NOAA, US Navy, NGA, GEBCO, Landsat/ Copernicus; copyright ZENRIN.

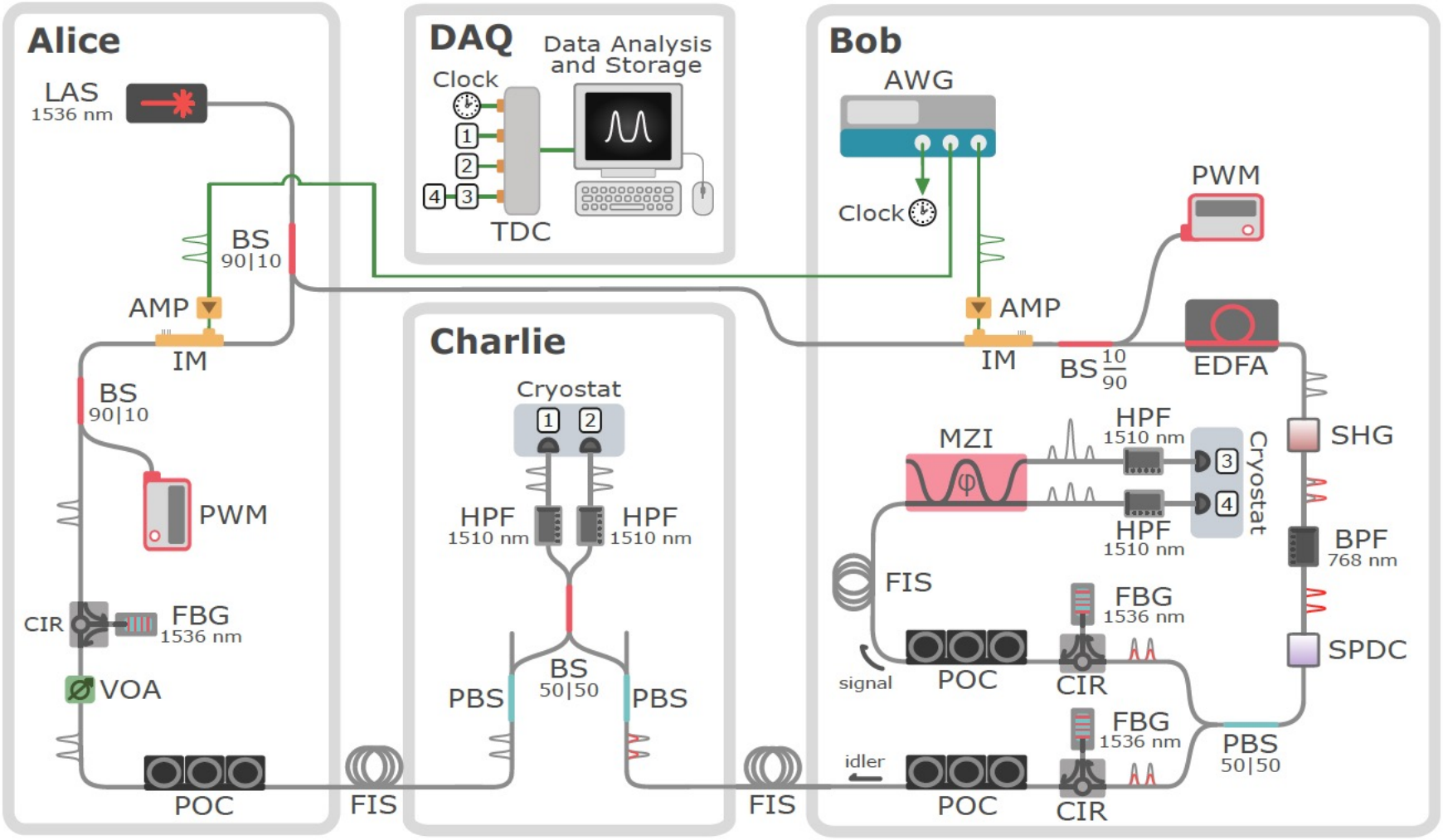
はじめに -- 各国・各研究グループの取り組み
アメリカ

2020/07/28 arXiv

"Teleportation Systems Towards a Quantum Internet"

https://arxiv.org/pdf/2007.11157.pdf

アメリカの量子情報ネットワークの拠点は、FermilabのFermilab Quantum Network (FQNET)と、Caltech のCaltech Quantum Network (CQNET) の二箇所である。CQNETが基礎的な研究・開発、プロトタイピングを行い、FQNETが DAOやHEP等の支援を受けて、量子インターネットの実現に向けた情報ネットワークの実践的な拡大・長距離化に取り組んでいる。この実験では、最新の nanowire single photon detecter を用い、90%以上の高い信頼性で、22km隔てた光ファイバー二点間の teleportationに成功した。



AMP = Amplifier

AWG = Arbitrary Waveform Generator

BS = Beam Splitter

BPF = Band Pass Filter
Bandwidth: 20 nm

CIR = Circulator

EDFA = Erbium Doped Fiber Amplifier

FBG = Fiber Bragg Grating

FIS = Fiber Spool

HPF = High Pass Filter

IM = Intensity Modulator

MZI = Mach-Zehnder Interferometer

LAS = Laser

PBS = Polarizing Beam Splitter

POC = Polarization Controller

PWM = Powermeter

SHG = Second Harmonic Generation

SPDC = Spontaneous Parametric Down Conversion

SNSPD = Superconducting Nanowire Single Photon Detector

TDC = Time-To-Digital Converter

VOA = Variable Optical Attenuator

はじめに -- 各国・各研究グループの取り組み
ヨーロッパ

2022/02/08 arXiv

“Satellite-based Quantum Information Networks: Use cases, Architecture, and Roadmap”

https://arxiv.org/pdf/2202.01817.pdf

French Space agency (CNES)を中心としたヨーロッパの研究機関と、民間の衛星通信企業からなるグループ。彼らは、量子情報ネットワークの中核は、衛星を使ったものになるというビジョンを持っている。当面、衛星と地上間でのentanglementの配布に注力するという。Quantum Memoryを使う。

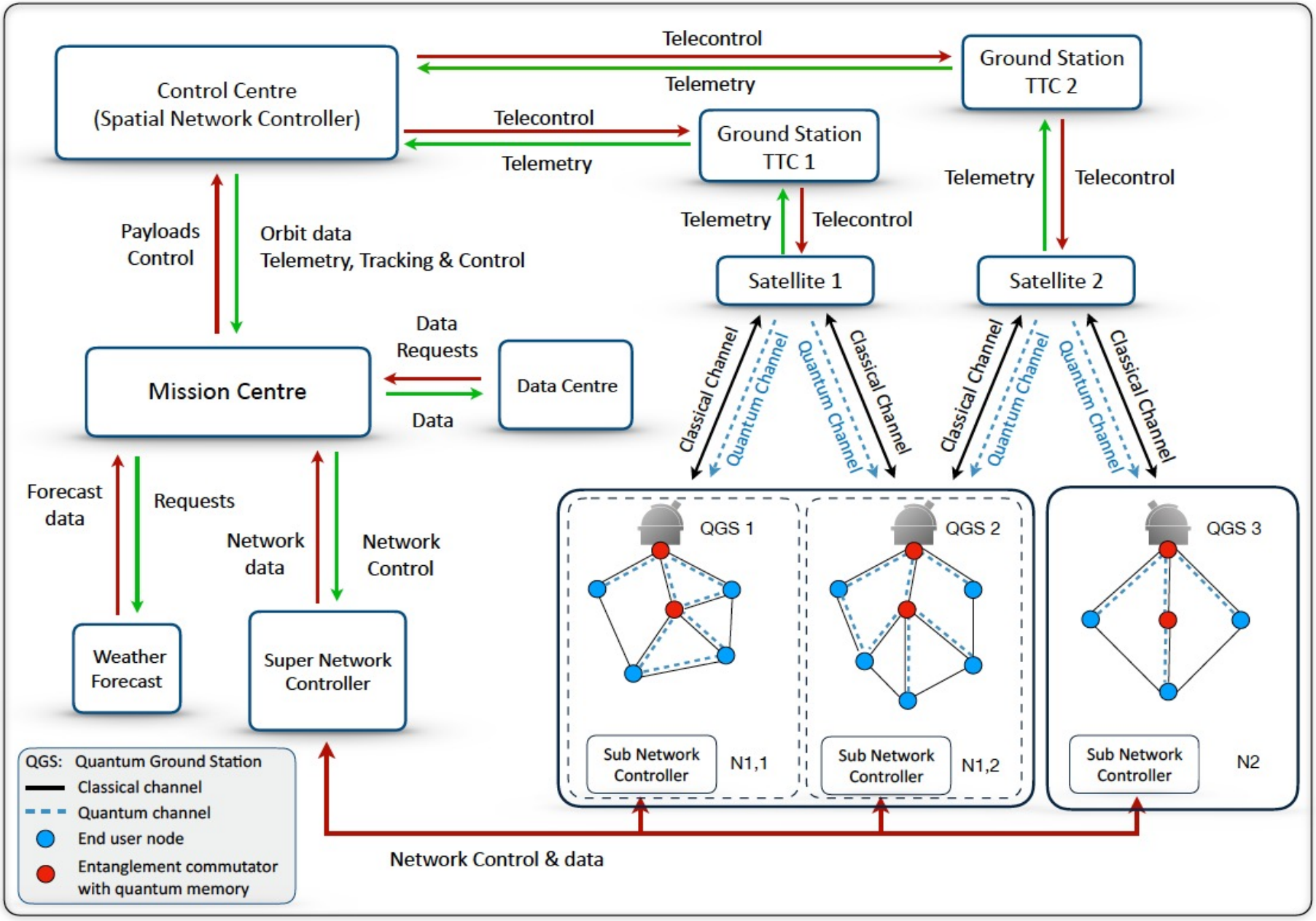


FIG. 2: Functionnal diagram of an integrated Quantum Information Network with a Space segment.

量子情報と通信技術
Agenda

はじめに

Part I　量子キー配布 BB84

Part II　量子テレポーテーション

Part III　量子通信の技術的基礎

- Entanglement Swapping
- Time-Bin Encoding

Part I

量子キー配布 BB84

Part Ⅰ 「量子キー配布 BB84」の概要

この章では、量子情報通信の基本的なプロトコルの一つである、「量子キー配布 BB84」 のロジック・考え方を紹介する。

少し変わった導入の仕方をしている。それは、BB84の骨組みの多くの部分は、量子論の知識を前提にしなくても理解できるというアプローチである。

ただ、このアプローチで利用されている、数度に渡るコイン投げで導入される「ランダムさ」は、それ自体はもちろん日常の世界に属するものだが、「ランダムさ」は、日常の世界と量子の世界を結ぶ重要なメッセージに他ならない。

Part Ⅰ 「量子キー配布 BB84」の概要

日常の世界の「コイン・トス」の振る舞いと、量子の世界の「量子コイン」の振る舞いとを区別することは難しいのだ。それは、同じものだ。

もっとも、コイン・トスで初等的にシミレート可能なBB84のロジックの基本部分と、キー配布にqubit を使うというより基本的なBB84のアイデアは関連しているが別のものだ。

小論では、後者の説明は、中間者攻撃に対する脆弱性から行われているのだが、初等的・古典論的な説明のスタイルに引きずられたところがあるように思う。

Part I　量子キー配布 BB84

Agenda

1. BB84をコインでシミレートする
2. BB84での共有キーの構成
3. BB84 コインからqubitへ

BB84をコインでシミレートする

ここでは、代表的な「量子キー配布」のプロトコルであるBB84をコインとコイントスでシミレートする。

コインを使った物理的な情報伝達なので、量子論の知識はいらない。

コインを使った物理的な情報伝達
基本的な流れ

- Aliceのエンコード
  Aliceは、受け取った情報1ビットを一つのコインに変換する。

- Aliceは、そのコインをBobに届ける。

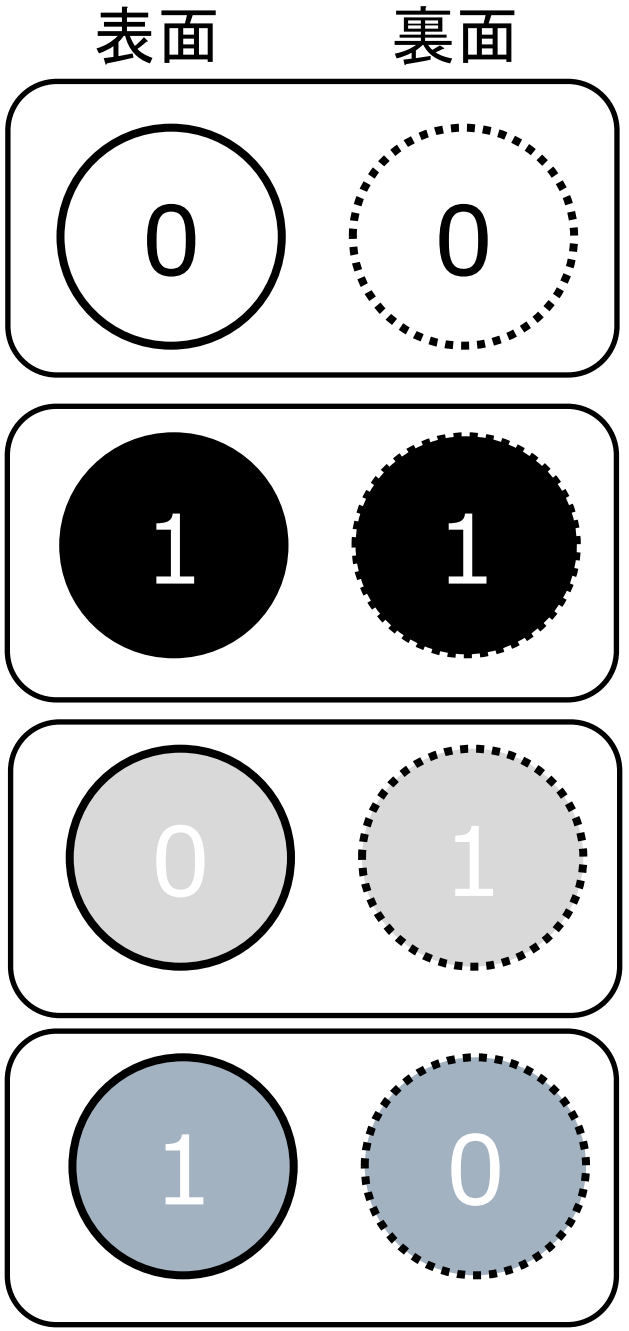
- Bobのデコード
  Bobは、受け取ったコインを情報1ビットに変換する

次のような4種類のコインを利用する

コインには、表面と裏面の区別があって、それぞれの面に、0または1の文字が刻まれている。

例えば、上から三番目のコインは、表面に0が、裏面に1が、刻まれている。

上から四番目のコインは、表面に1が、裏面には0が、刻まれている。

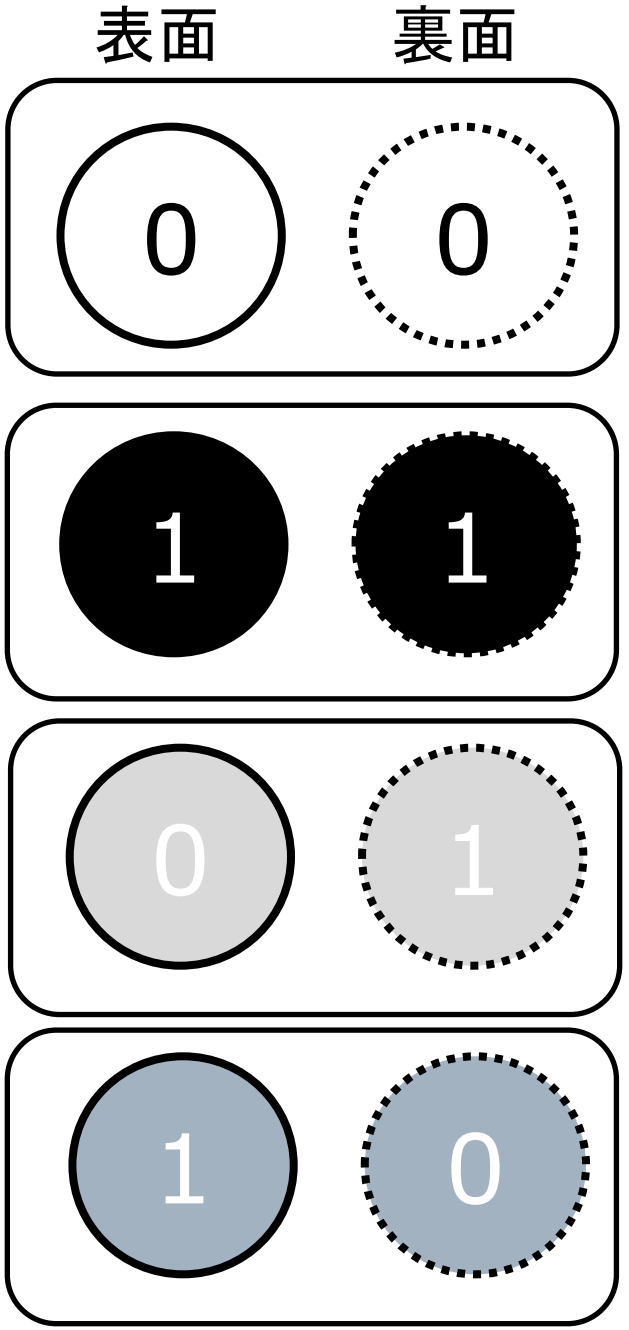


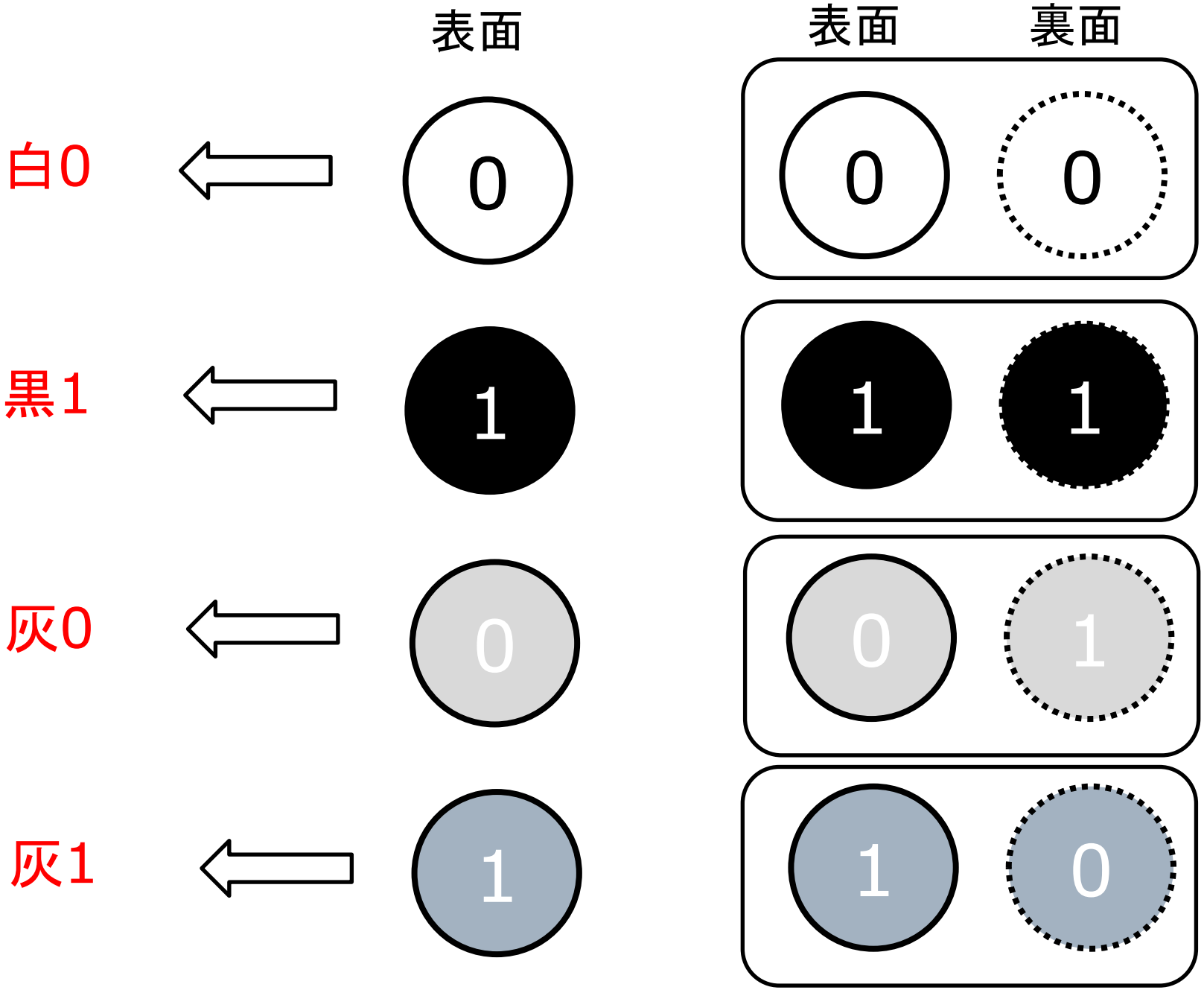
次のような4種類のコインを利用する

コインには、白、黒、二つの灰色の色がある。

コインの色と、表面に刻まれた数字で、四つのコインの区別ができる。

それぞれのコインの名前を、「白0」、「黒1」、「灰0」、「灰1」としよう。




表面
表面
裏面
白0
0
0
0
黒1
1
1
1
灰0
0
0
1
灰1
1
1
0

Aliceが行うエンコードと
Bobが行うデコード

Aliceが行うエンコードとBobが行うデコード
三つのコイントス

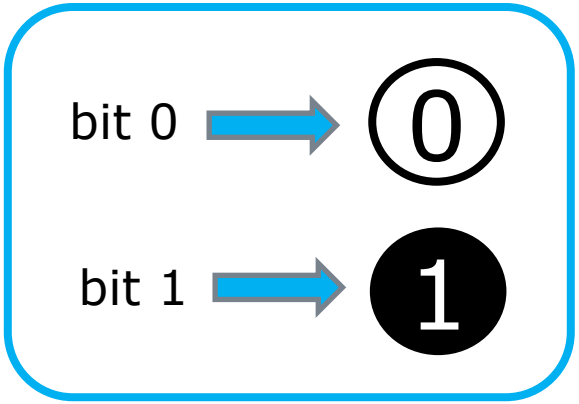
- Aliceが受け取った 入力1bitは、あるルールでコインにエンコードされる。Aliceのエンコードには、二種類のエンコード・ルールがある。
  - どのエンコード・ルールが選ばれるかは、コイントスでランダムに決められる。
- Bobにも二種類のデコード・ルールがある。
  - どのデコード・ルールが選ばれるかは、コイントスでランダムに決められる。
- Bobは、ある場合には、うけとったコインをそのまま、ある場合にはコインを他のコインに変えてからデコードする。
  - Bobは、最終的に与えられたコインをトスして、でた面の数字を出力とする。

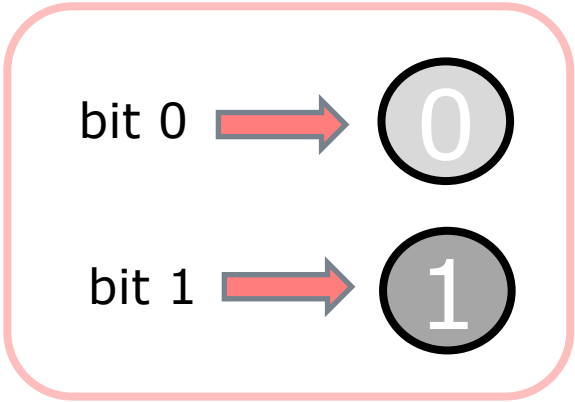
Aliceのエンコード・ルールの二つのタイプ
コイントス1

- Type I
  - bit 0をコイン「白0」にエンコードする
  - bit 1をコイン「黒1」にエンコードする

コイントス1

- Type II
  - bit 0をコイン「灰0」にエンコードする
  - bit 1をコイン「灰1」にエンコードする

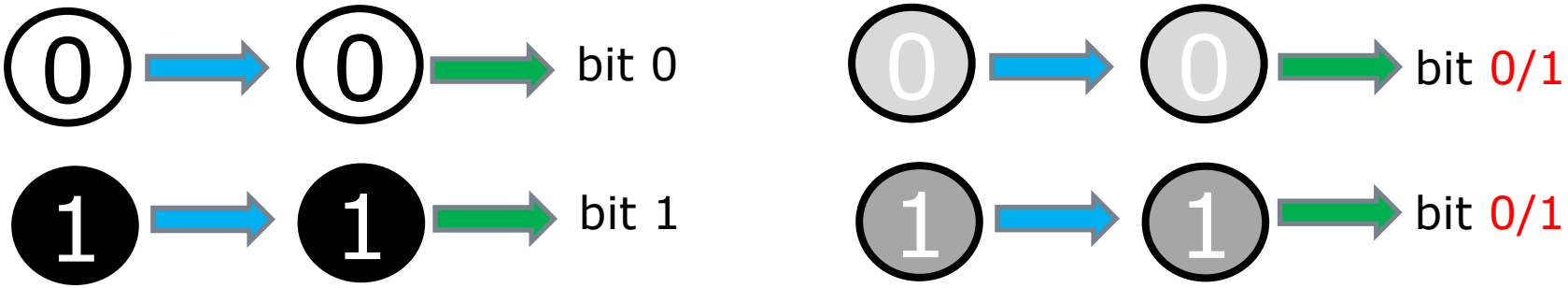




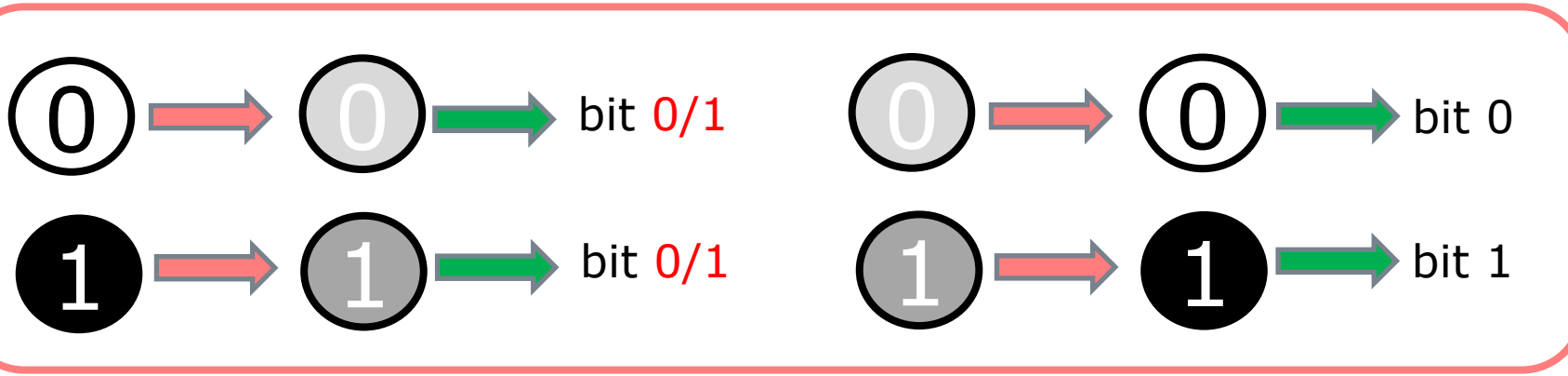
Type I をストレート、Type II をミクストと呼ぼう。

Bobのデコード・ルールの二つのタイプ
コイントス2

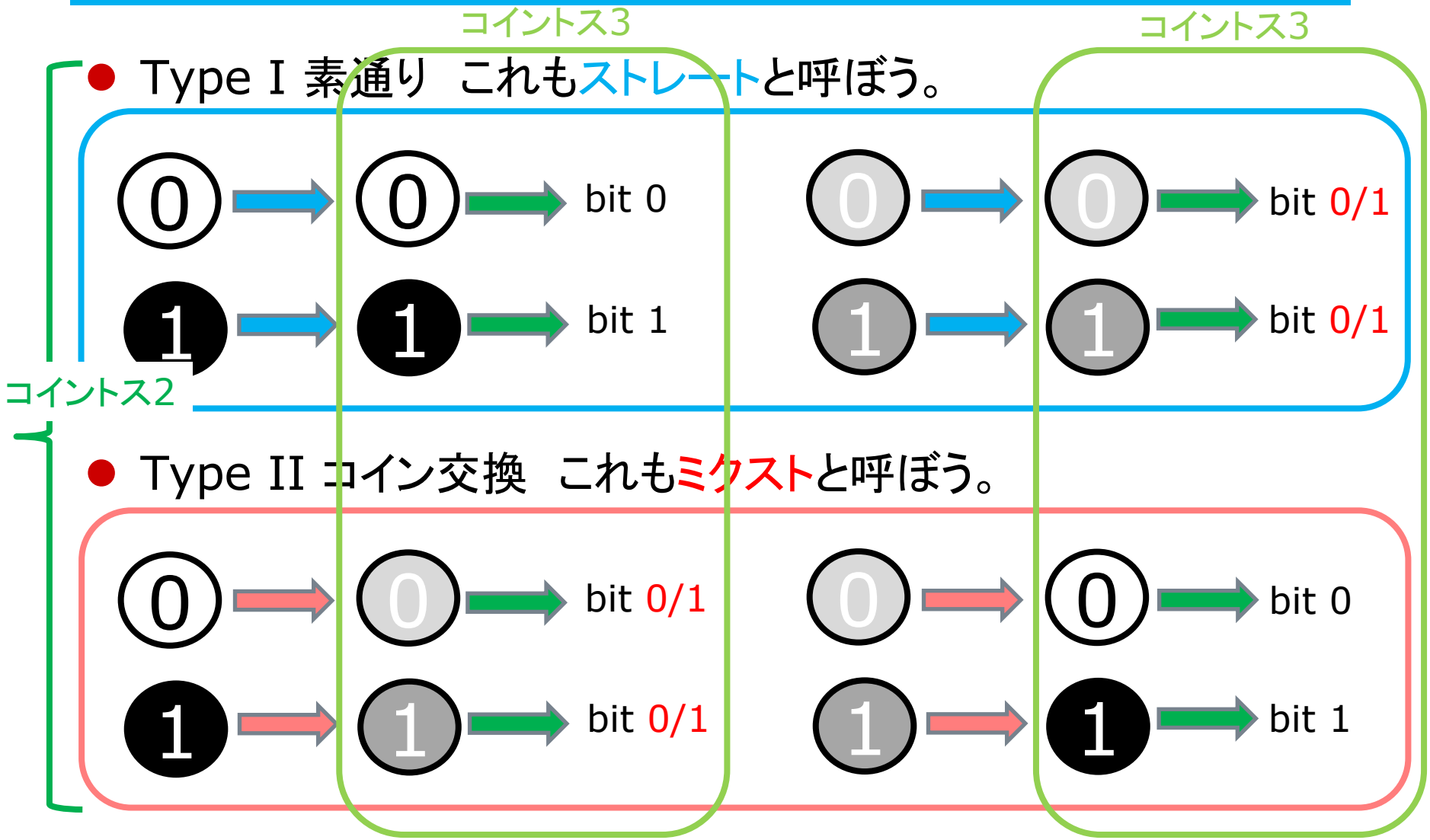
- Type I 素通り　これもストレートと呼ぼう。



- Type II コイン交換　これもミクストと呼ぼう。

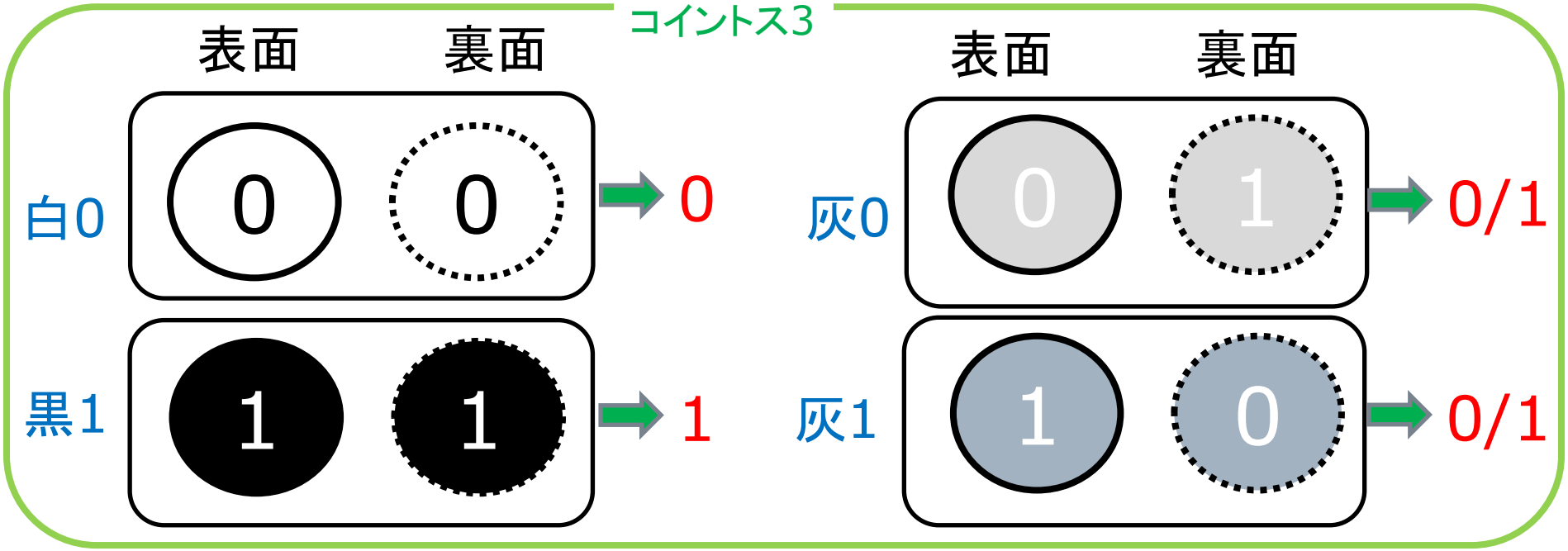


Bobのデコード・ルールの二つのタイプ
コイントス2 / コイントス3



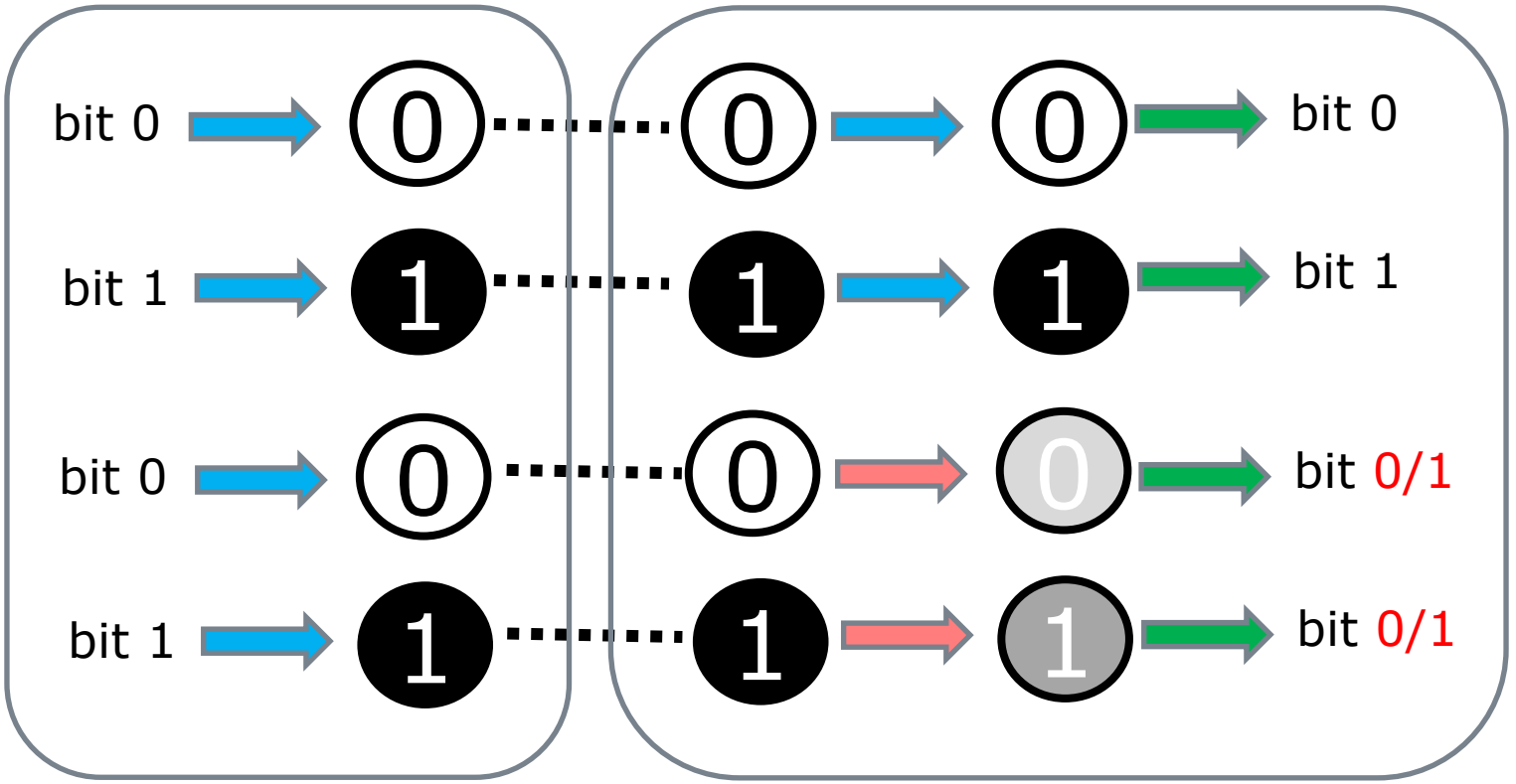
Bobの最後のデコードの例
コイントス3

- コイン「白0」の場合、両面が0なので、必ず0が出力される。
- コイン「黒1」の場合、両面が1なので、必ず1が出力される。
- コイン「灰0」の場合、1がでる確率は1/2、0が出る確率は1/2。
- コイン「灰1」の場合、1がでる確率は1/2、0が出る確率は1/2。

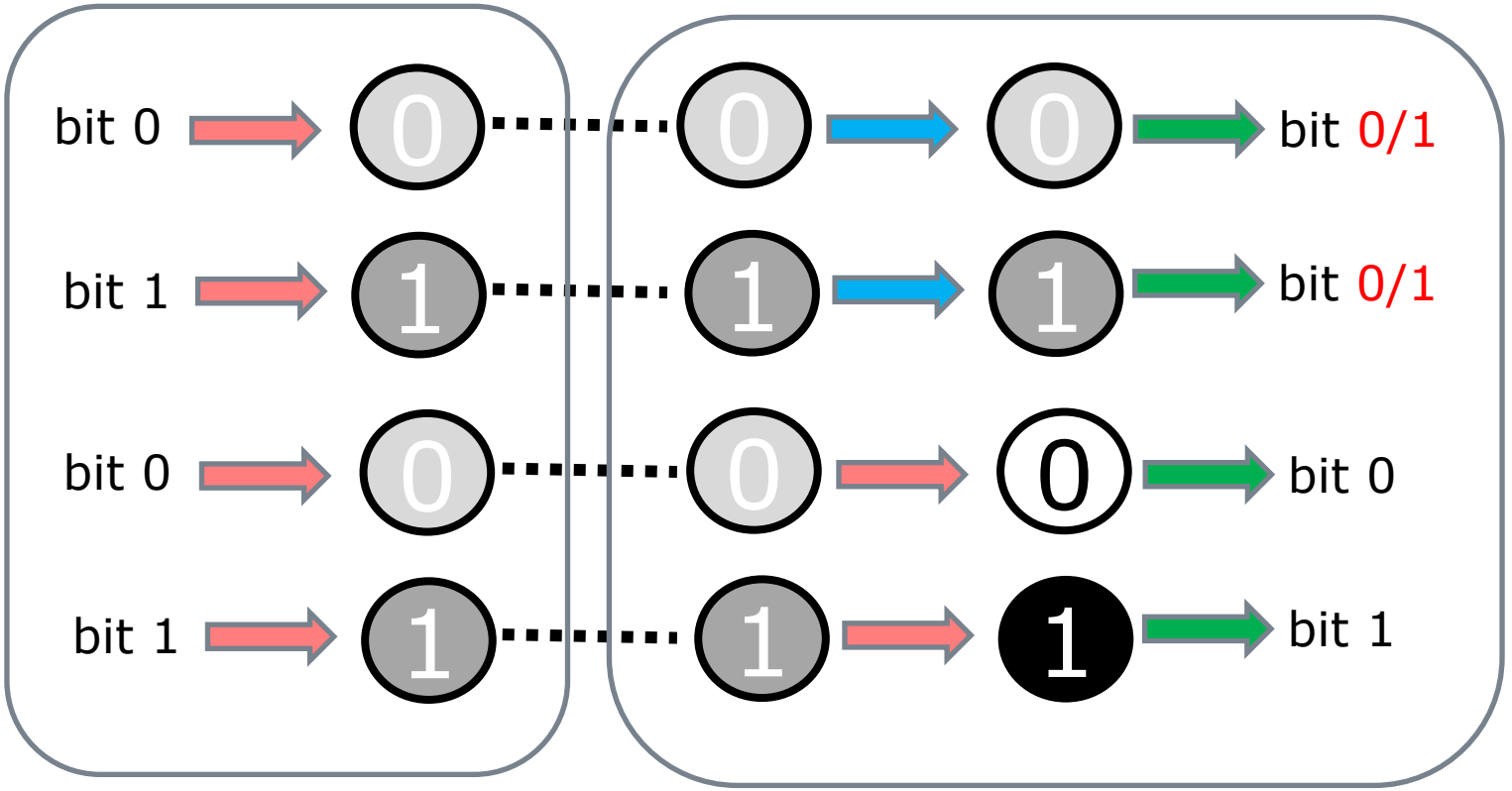


三つのコイントスをへて
AliceからBobに送られる情報

エンコードとデコードの例
Alice エンコード　ストレート



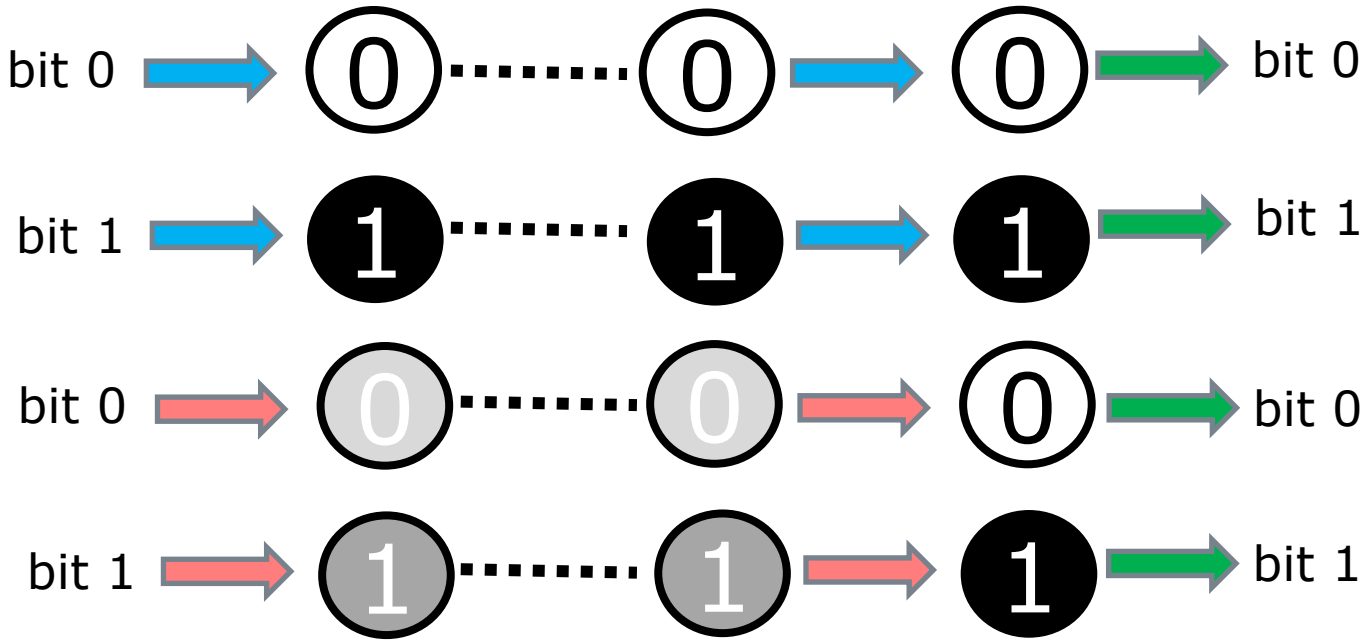
エンコードとデコードの例
Alice エンコード　ミクスト



Alice エンコード
ミクスト

Bob デコード

入力が正しく出力されるのは、次の場合である



エンコードもデコードもストレートか、あるいは、
エンコードもデコードもミクストの場合である。

BB84での共有キーの構成

Aliceが行うこととBobが行うこと

共有キーの構成 サンプル

- Aliceは、ランダムなビット列を準備する。

Aliceの送信ビット　**0　1　1　0　0　….　0　1　0　1**

共有キーの構成 サンプル

- Aliceは、ランダムなビット列を準備する。
- Aliceは、ランダムなビット列を、コインにエンコードする。この時、エンコードの方式として、「ストレート」を選ぶか「ミクスト」を選ぶかは、コイントスでランダムに決める。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x

共有キーの構成 サンプル

- Aliceは、ランダムなビット列を準備する。
- Aliceは、ランダムなビット列を、コインにエンコードする。この時、エンコードの方式として、「ストレート」を選ぶか「ミクスト」を選ぶかは、コイントスでランダムに決める。
- Bobのデコードでは、まず、Aliceから受け取ったコインを、別のコインに変換する。この変換に、「ストレート」を選ぶか、「ミクスト」を選ぶかは、コイントスでランダムに決める。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x

共有キーの構成 サンプル

- Aliceは、ランダムなビット列を準備する。
- Aliceは、ランダムなビット列を、コインにエンコードする。この時、エンコードの方式として、「ストレート」を選ぶか「ミクスト」を選ぶかは、コイントスでランダムに決める。
- Bobのデコードでは、まず、Aliceから受け取ったコインを、別のコインに変換する。この変換に、「ストレート」を選ぶか、「ミクスト」を選ぶかは、コイントスでランダムに決める。
- Bobは、このコインをコイントスして、表の数字を読み取り、それをデコードの出力とする。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

共有キーの構成 サンプル

- Aliceは、ランダムなビット列を準備する。
- Aliceは、ランダムなビット列を、コインにエンコードする。この時、エンコードの方式として、「ストレート」を選ぶか「ミクスト」を選ぶかは、コイントスでランダムに決める。
- Bobのデコードでは、まず、Aliceから受け取ったコインを、別のコインに変換する。この変換に、「ストレート」を選ぶか、「ミクスト」を選ぶかは、コイントスでランダムに決める。
- Bobは、このコインをコイントスして、表の数字を読み取り、それをデコードの出力とする。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

AliceとBobが
お互い知らないこと

- Aliceが送ったビットを、Bobは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

AliceとBobが
お互い知らないこと

- Aliceが送ったビットを、Bobは知らない。
- Aliceが使ったエンコード方法を、Bobは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

AliceとBobが
お互い知らないこと

- Aliceが送ったビットを、Bobは知らない。
- Aliceが使ったエンコード方法を、Bobは知らない。
- Bobが使ったエンコード方法を、Aliceは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

AliceとBobが
お互い知らないこと

- Aliceが送ったビットを、Bobは知らない。
- Aliceが使ったエンコード方法を、Bobは知らない。
- Bobが使ったデコード方法を、Aliceは知らない。
- Bobが受け取ったビットを、Aliceは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

AliceとBobの情報の共有

AliceとBobの情報の共有

- Aliceが送ったビットを、Bobは知らない。
- Aliceは、使ったエンコード方法を、Bobに伝える。
- Bobは、使ったデコード方法を、Aliceに伝える。
- Bobが受け取ったビットを、Aliceは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

AliceとBobの情報の共有

- Aliceが送ったビットを、Bobは知らない。
- Aliceは、使ったエンコード方法を、Bobに伝える。
- Bobは、使ったデコード方法を、Aliceに伝える。
- Bobが受け取ったビットを、Aliceは知らない。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

AliceとBobの情報の共有

- Aliceが送ったビットを、Bobは知らない。
- Aliceは、使ったエンコード方法を、Bobに伝える。
- Bobは、使ったデコード方法を、Aliceに伝える。
- Bobが受け取ったビットを、Aliceは知らない。

AliceとBobは、各ビットのエンコード方法と
デコード方法の情報を共有する。

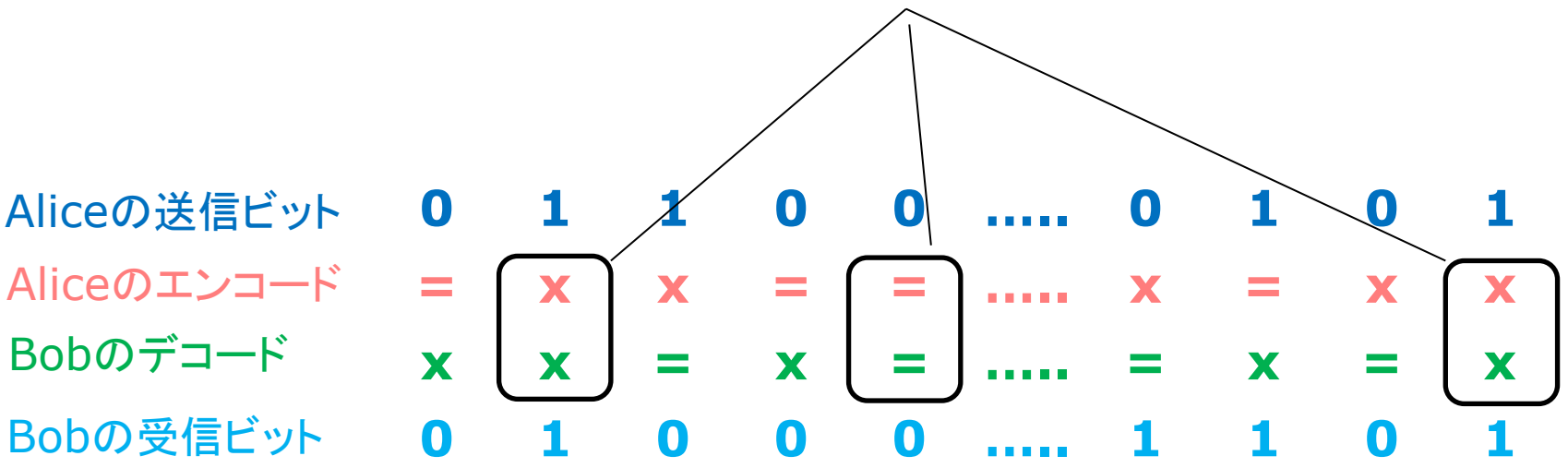
Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	0	1	0	0	0	.....	1	1	0	1

共有キーの構成

共有キーの構成

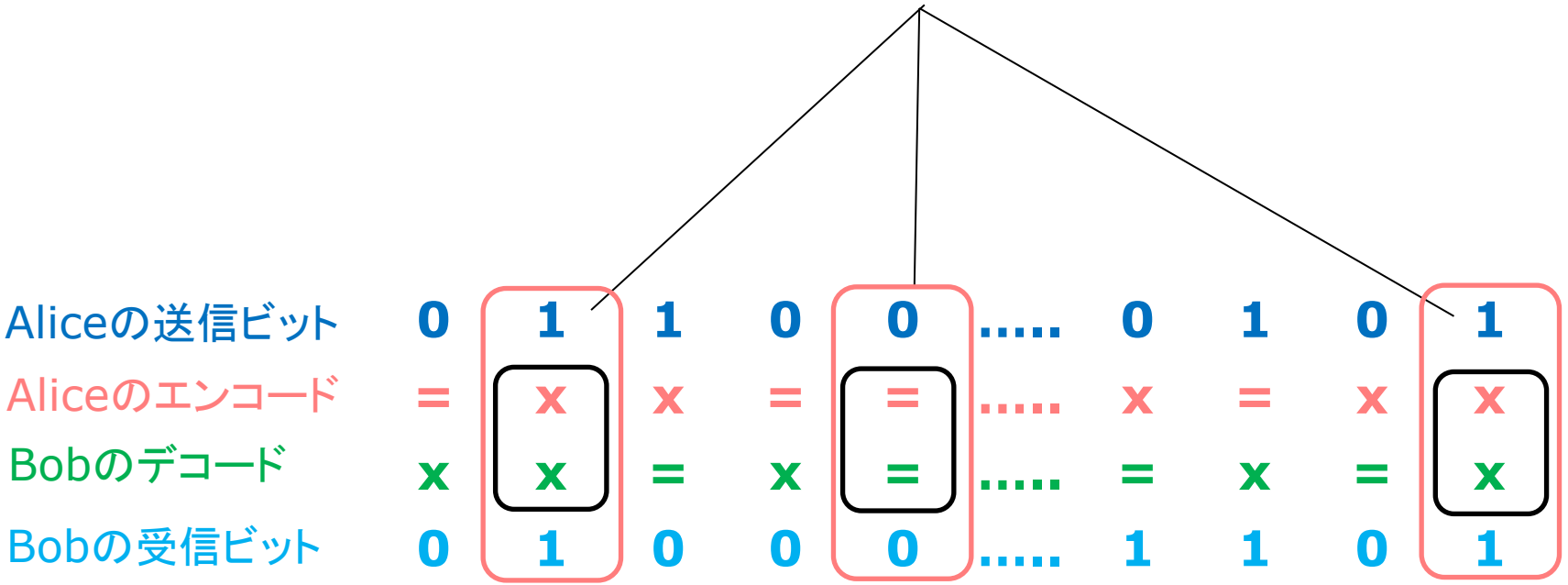
- AliceとBobが共有する、エンコード・デコードの情報で、エンコードのタイプとデコードのタイプが等しいものをピックアップする。

Aliceのエンコードの方法とBobのデコードの方法が等しいものをピックアップする。



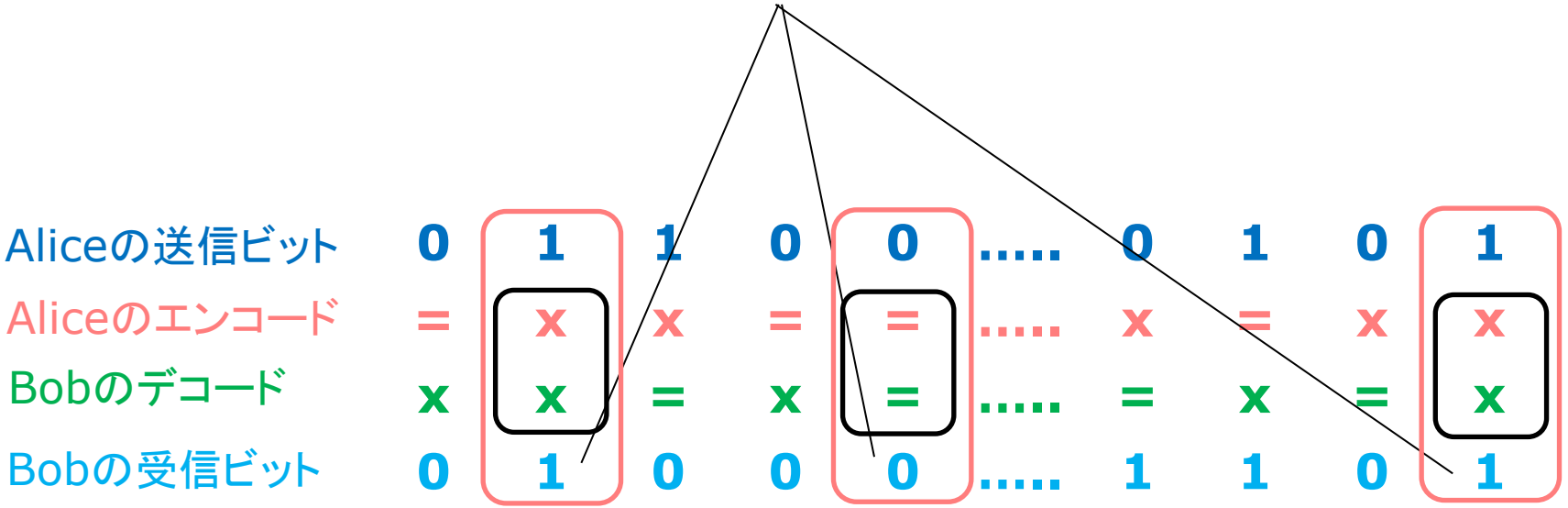
共有キーの構成

- AliceとBobが共有する、エンコード・デコードの情報で、エンコードのタイプとデコードのタイプが等しいものをピックアップする。
- ピックアップしたコラムの、Aliceの送信ビットを見る。



共有キーの構成

- AliceとBobが共有する、エンコード・デコードの情報で、エンコードのタイプとデコードのタイプが等しいものをピックアップする。
- ピックアップしたコラムの、Aliceの送信ビットを見る。
- それは、Bobの受信ビットと一致しているはずである。



共有キーの構成

- AliceとBobは、二人が共有しているエンコード・デコードの情報を公開しても構わない。
- 第三者が、公開されたエンコード・デコードの情報から、共有キーを推測することはできない。Aliceがどのようなビットを入力したのかは、誰にもわからないから。
- Bobだけが、エンコード・デコードの情報から、Aliceの入力ビットがBobが受信したビットに等しいことを知る。
- それが、AliceとBobの共有キーになる。

Aliceの送信ビット	?	?	?	?	?	.....	?	?	?	?
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	?	?	?	?	?	.....	?	?	?	?

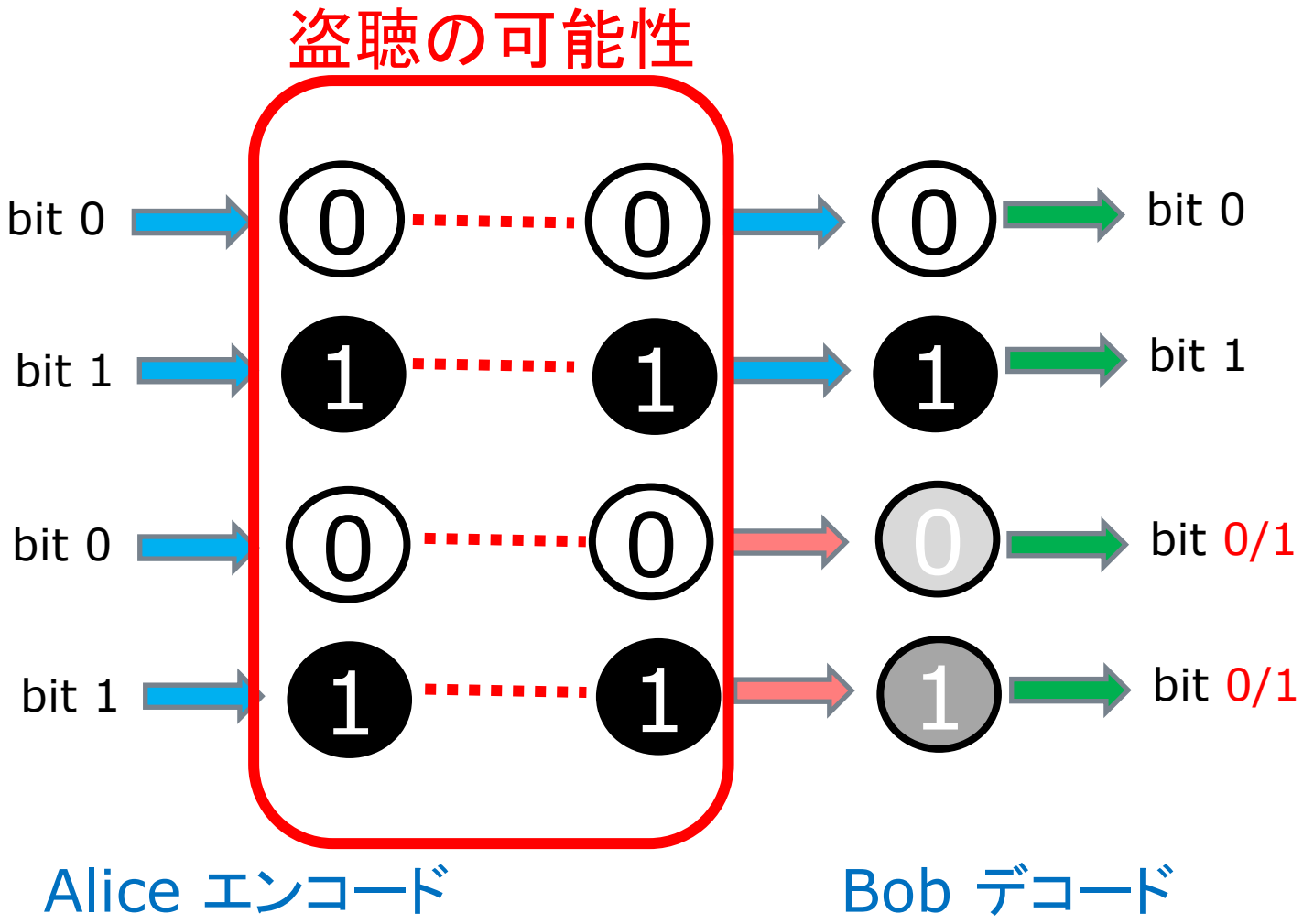
共有キーの構成は、安全に行われるか？

AliceとBobの間の、こうした共有キーの構成のプロトコルは、安全だろうか？

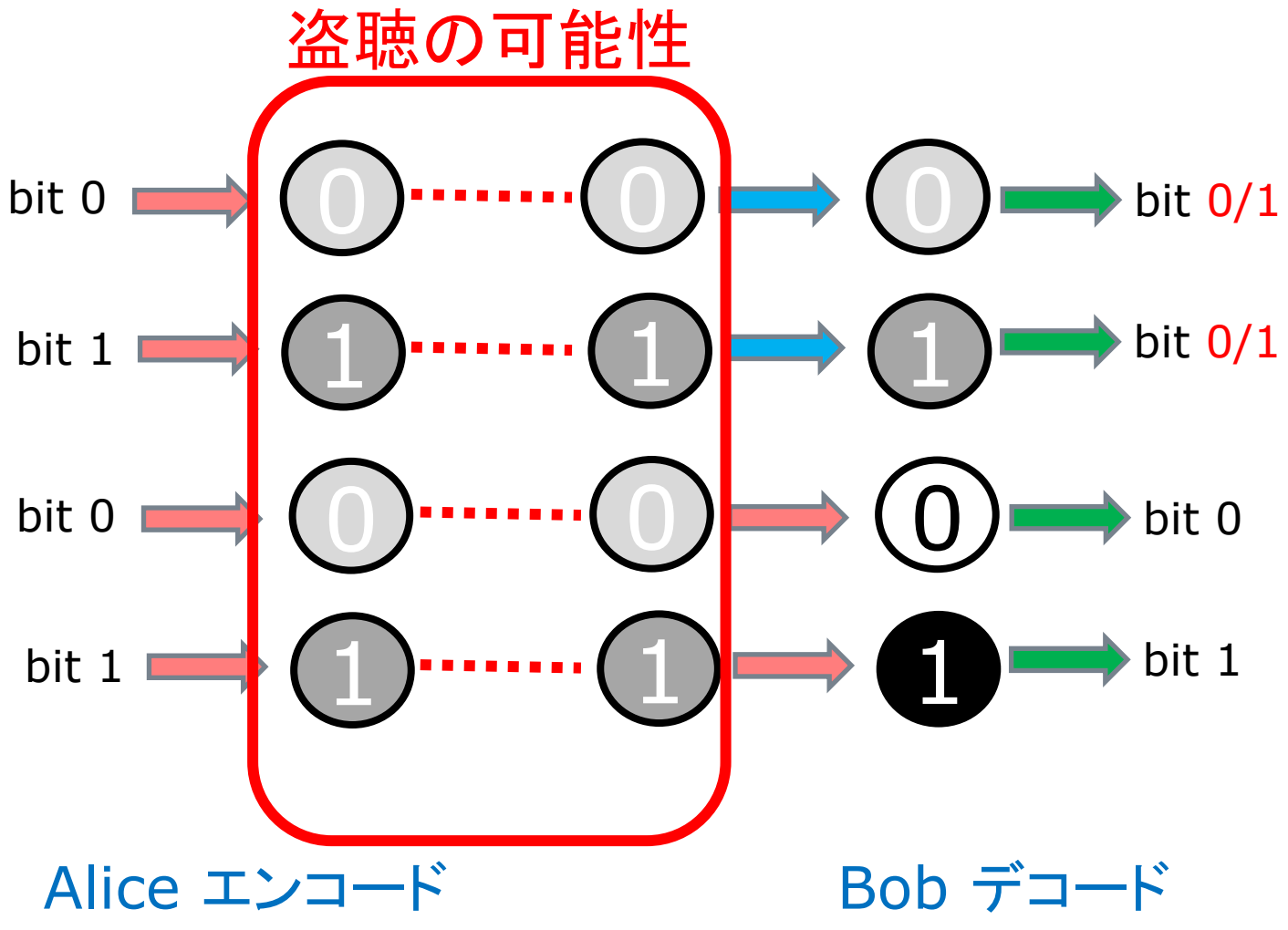
それについては、次に考察する。

コインによる通信の脆弱性

コインでの通信には脆弱性がある



コインでの通信には脆弱性がある



中間者攻撃

- 中間攻撃者Eveは、AliceからBobに送られるコインをBobが受け取る前に密かに奪取して、コインの表の数字(Aliceの送信ビット)を記録し、同じコインを改めてBobに送る。Bobは情報が盗まれたことに気づかない。

盗聴されたデータ

Aliceの送信ビット	0	1	1	0	0	….	0	1	0	1
Aliceのエンコード	=	x	x	=	=	….	x	=	x	x
Bobのデコード	x	x	=	x	=	….	=	x	=	x
Bobの受信ビット	?	?	?	?	?	….	?	?	?	?

中間者攻撃

- 中間攻撃者Eveは、AliceからBobに送られるコインをBobが受け取る前に密かに奪取して、コインの表の数字(Aliceの送信ビット)を記録し、同じコインを改めてBobに送る。Bobは情報が盗まれたことに気づかない。

- 攻撃者は、公開されたエンコード・デコードの情報から、たやすく共有キーを知ることができる。

Aliceの送信ビット	0	1	1	0	0	.....	0	1	0	1
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	?	?	?	?	?	.....	?	?	?	?

物理的コインによる
量子暗号のシミレーションは失敗する

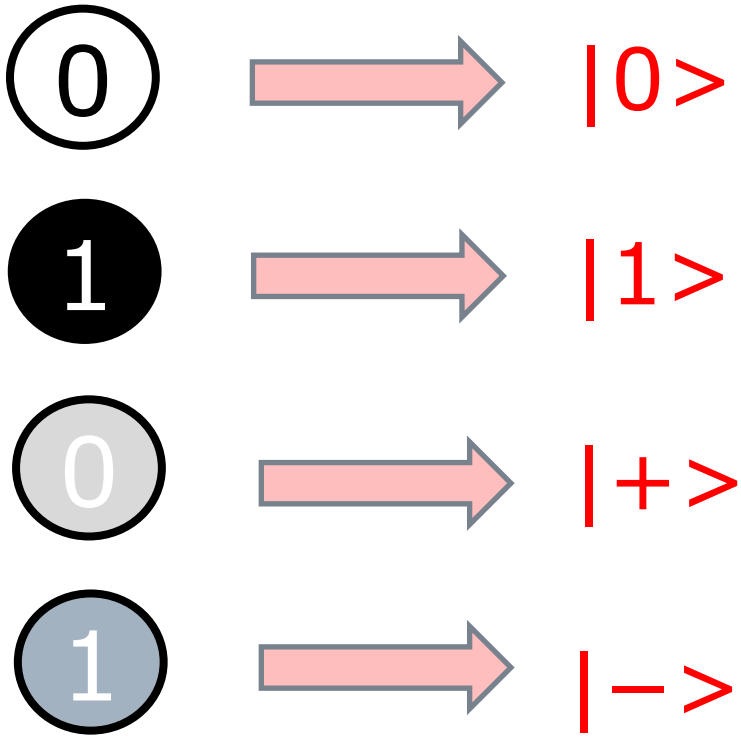
- 量子暗号のエンコード・デコードのシミレーションは、物理的コインでも可能である。
- 量子暗号の共有キーの構成のシミレーションは、物理的コインでも可能である。
- ただ、AliceからBobに、物理的コインを渡すというスタイルでは、中間者攻撃により、共有キーの秘密は破られる。

- それでは、この問題に、量子暗号はどう対処しているのであろうか？

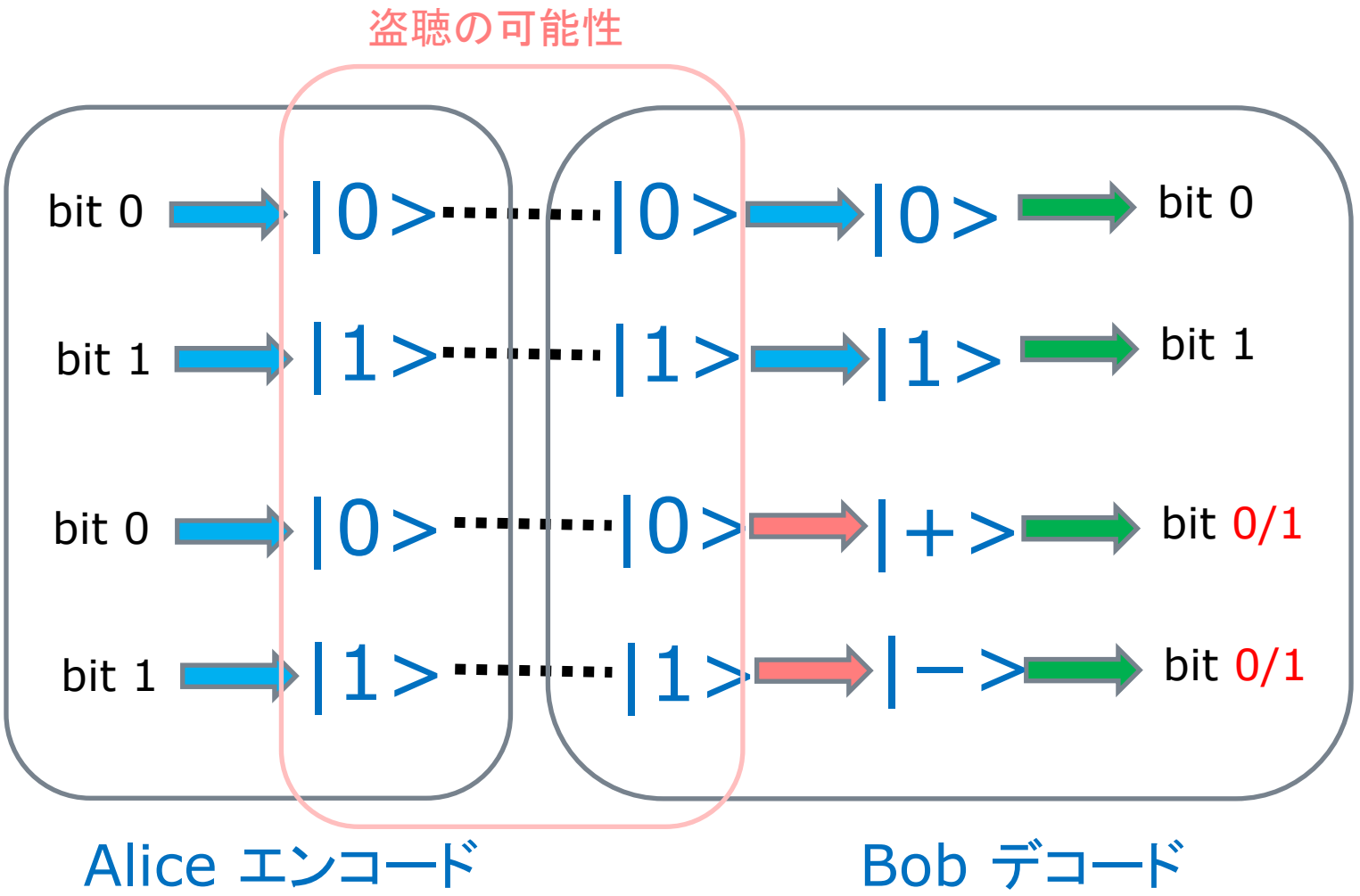
BB84　コインからqubitへ

コインからqubitへ

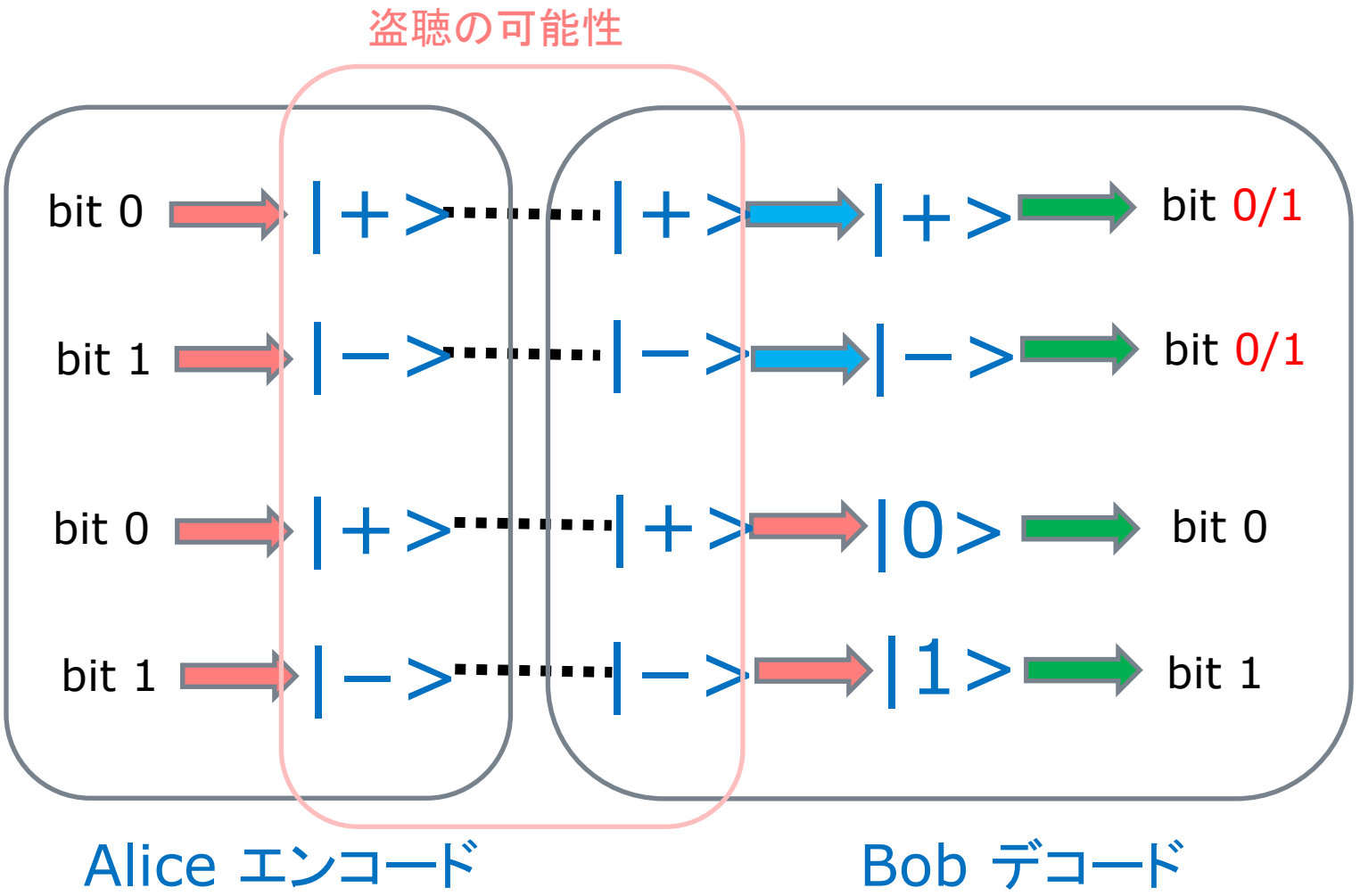
メッセージの担い手を、つぎのように、
コインからqubitに切り替える。



qubit バージョン


盗聴の可能性
bit 0
|0>
|0>
|0>
bit 0
bit 1
|1>
|1>
|1>
bit 1
bit 0
|0>
|0>
|+>
bit 0/1
bit 1
|1>
|1>
|−>
bit 0/1
Alice エンコード
Bob デコード

qubit バージョン


盗聴の可能性
bit 0
|+>
|+>
|+>
bit 0/1
bit 1
|−>
|−>
|−>
bit 0/1
bit 0
|+>
|+>
|0>
bit 0
bit 1
|−>
|−>
|1>
bit 1
Alice エンコード
Bob デコード

攻撃者Eveが行うべきこと

メッセージの担い手がコインなら、中間攻撃者Eveは、AliceからBobに送られるコインをBobが受け取る前に密かに奪取して、コインの表の数字（Aliceの送信ビット）を記録し、同じコインを改めてBobに送ればいい。

メッセージの担い手がコインからqubitに変わっても、Eveが行うべきことは、基本的には、Aliceから送られたqubit |X>から、Aliceの送信ビットの情報を盗んで、qubit |X>をBobに送ることである。

Eveは、盗聴した|X>から
何を知ることができるか？

- Eve は、Aliceが送った|X>が何かを知り、|X>をBobに送るためには、まず |X>を観測しなければならない。
- 観測結果が 0 の場合、|X>は |0>,|+>,|−>の可能性があり、Aliceの送信ビットは、0,1 の可能性がある。
- 観測結果が 1 の場合、|X>は |1>,|+>,|−>の可能性があり、Aliceの送信ビットは、0,1 の可能性がある。
- Eveは、|X>から、Aliceのエンコードの形式も、Aliceの送信ビットも、正確には知り得ない。

Aliceの送信ビット	?	?	?	?	?	.....	?	?	?	?
Aliceのエンコード	=	x	x	=	=	.....	x	=	x	x
Bobのデコード	x	x	=	x	=	.....	=	x	=	x
Bobの受信ビット	?	?	?	?	?	.....	?	?	?	?

このプロトコルは、攻撃に対して安全である

- Aliceの送信ビットが、0か1かの Eveの推測が正しい確率は、1/2 である。
- Aliceの行ったエンコードの方式が分からないと、|X>の形は分からない。エンコードには、「ストレート」と「ミクスト」の二つがあるので、そのどちらかというEveの推測が正しい確率は 1/2 である。
- その両方の推測が正しい場合に、AliceとBobが共有するビットの正しい推測ができる。AliceとBobが共有する 1 ビットについて、盗聴によってEveが正しい推測を行う確率は、 1/2 x 1/2 = 1/4 である。
- AliceとBobが共有するビットの桁数が大きくなるにつれ、正しい情報が盗まれる可能性は、ゼロに近づく。

Part II

量子テレポーテーション

Part II 「量子テレポーテーション」の概要

量子情報通信の中心的な機能は、あるノード上のqubitが持つ情報を、ネットワークをまたいで、正確に他のノードに送ることにある。

「量子テレポーテーション」は、まさにその機能を担う、量子情報通信の中核技術である。

「量子テレポーテーション」は、通信ノードの両端が、エンタングルメント状態にあることを前提とする。実践的には、量子テレポーテーション技術は、各ノードへのエンタングルメント・ペアの配布技術と一体のものである。

Part II 「量子テレポーテーション」の概要

この章では、量子テレポーテーション回路の働きを、「計算」で確認することを目標にする。

エンタングルメント状態を生成する Bell State Gate (BSG) と、エンタングルメント状態を観測する Bell Measure Gate (BMG)を導入する。

また、量子テレポーテーション回路を、BSG回路とBMG回路で再構成する。それらは、次章のEntanglement Swapping の基礎となる。

Part II　量子テレポーテーション
Agenda

1. エンタングルメントを利用した量子通信
2. qubitのテンソル積 計算練習
3. 量子テレポーテーションを計算する
4. Bell State GateとBell Measure Gate
5. Bell State Gate とBell Measure Gateで
   量子テレポーテーション回路を記述する

量子テレポーテーション

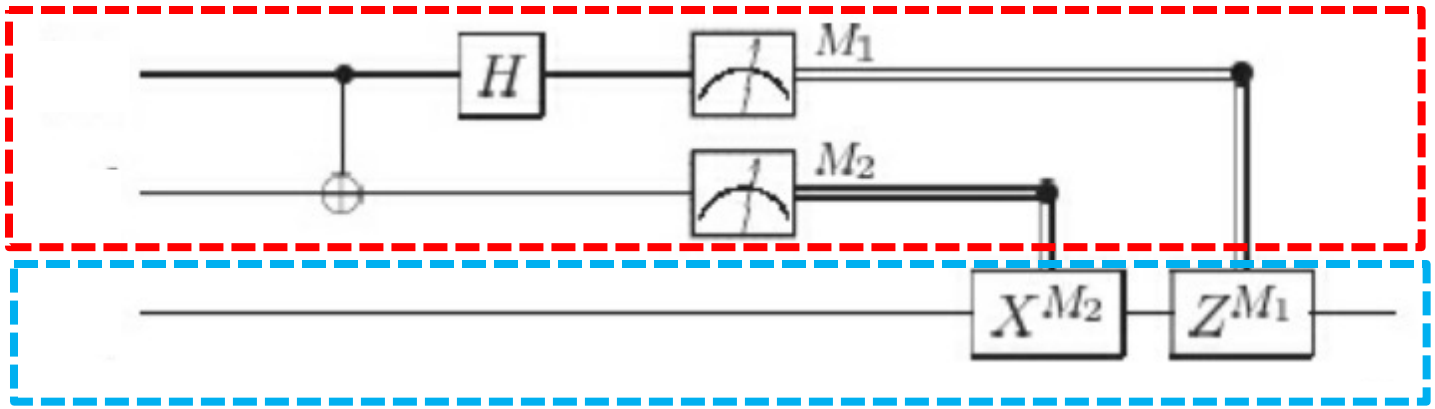
-- エンタングルメントを利用した量子通信 --

量子テレポーテーション

AliceとBobがエンタングル状態にあるとき、簡単な量子回路で、Aliceのもつqubitの状態をBobにそのまま送ることができる。それを「量子テレポーテーション」という。

量子テレポーテーション回路

Alice

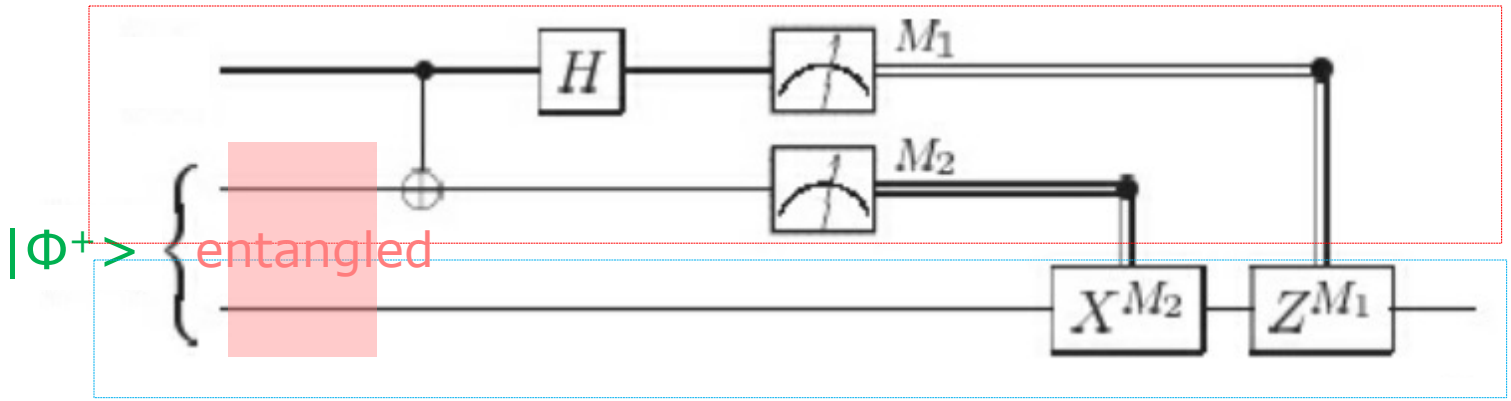


Bob

量子テレポーテーション回路は、こんな形をしている。
赤線部がAlice側、
青線部がBob側である。

AliceとBobはエンタングルしている

Alice

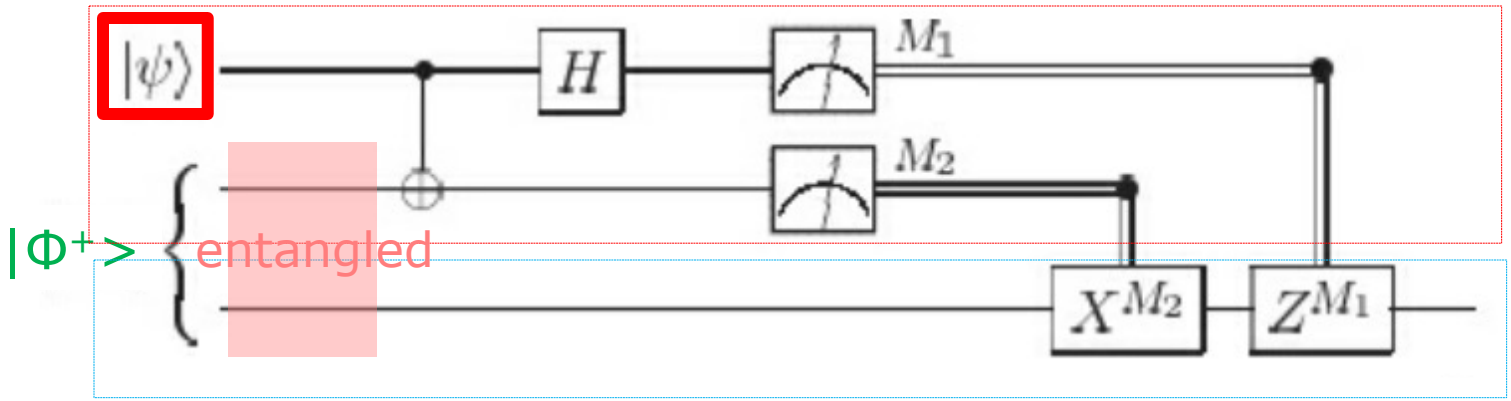


Bob

この回路では、AliceとBobは、エンタングル状態にあることが前提されている。（図の$|\Phi^+\rangle$がそれを表している。）

テレポーテーション

Alice

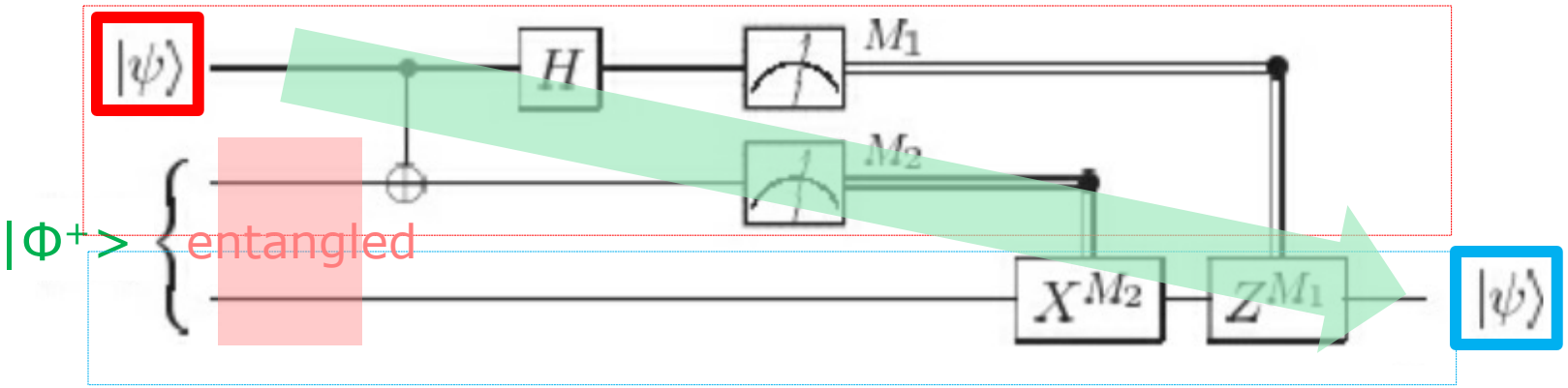


Bob

Alice側に、qubit $|\psi>$ が置かれた時、

テレポーテーション

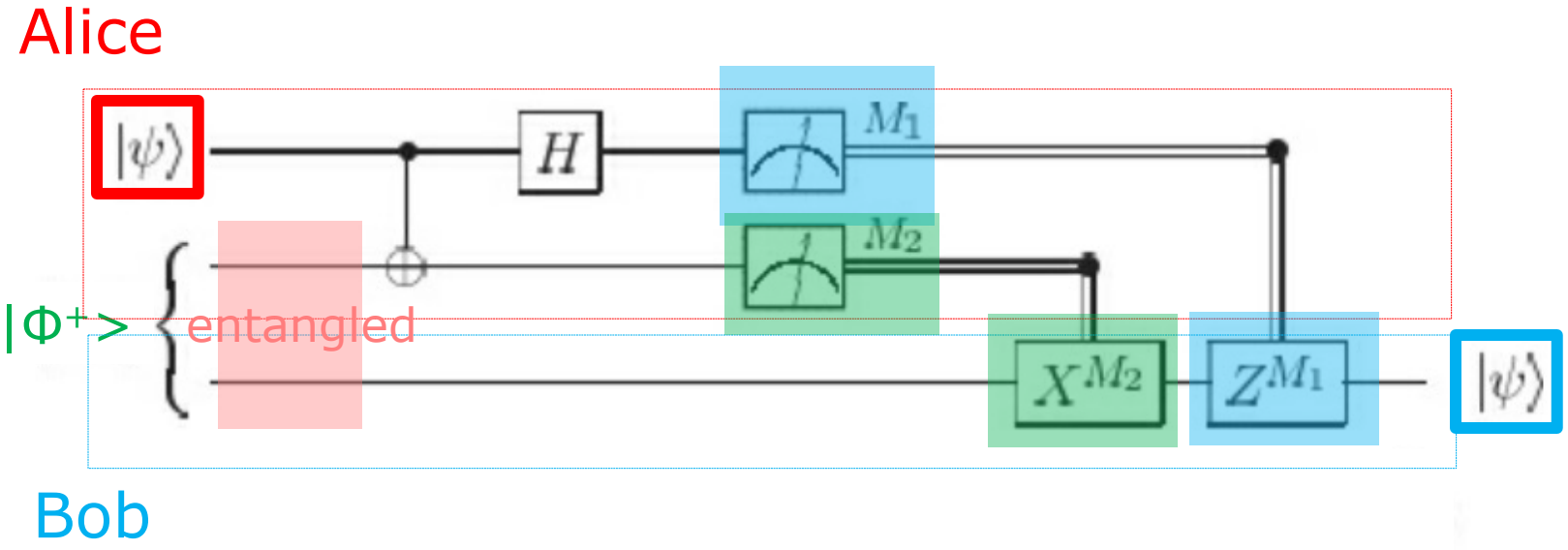
Alice



Bob

Alice側に。qubit $|\psi>$ が置かれた時、
Bob側に、　qubit $|\psi>$ が転送される。
この回路図は、横長に書かれているが、通信が行われるのは、
AliceからBobへ、縦方向に行われる

Alice側の観測で
Bob側のゲートをコントロールする



回路の働きを、もう少し詳しくみておこう。
Aliceは、第一qubitをM1で観察して、0か1の値を得る。
その値は、Bob側に伝えられ、Zゲートをコントロールする。
Aliceは、第二qubitをM2で観察して、0か1の値を得る。
その値は、Bob側に伝えられ、Xゲートをコントロールする。

いくつかの疑問

第一。量子テレポーテーションは、光より早く量子状態を送ることができるのだろうか？

これに対する答えは、明確にノーだ。テレポーテーションを実行するためには、Aliceは観測結果を、古典的な通信路でBobに送らなければならないのだから。

第二。量子テレポーテーションは、未知の量子状態のコピーを禁じたNo Cloning定理を破ることにならないか？

これについても、答えはノーだ。Bobのもとで、量子状態は再現されるのだが、Aliceのもとにあったオリジナルの量子状態は、Aliceの観測によって、|0>か|1>かの状態に変わって、失われている。

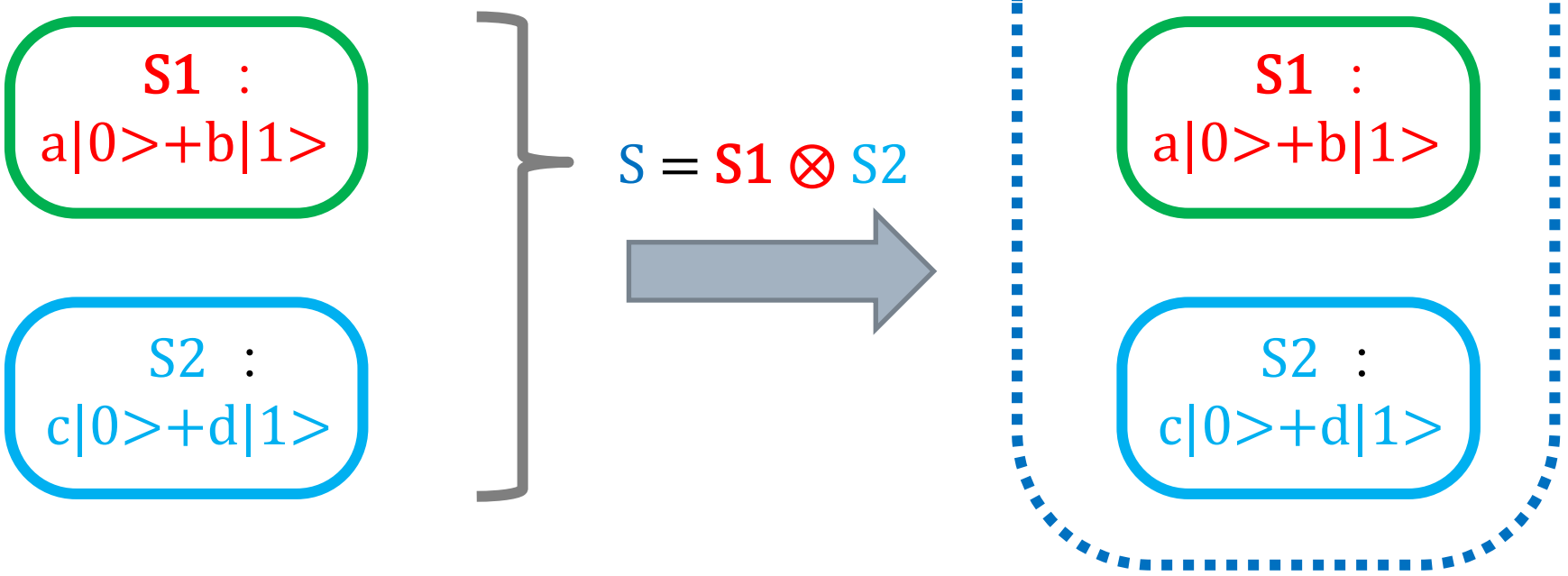
量子テレポーテーションの為の qubitのテンソル積 計算練習

qubitのテンソル積

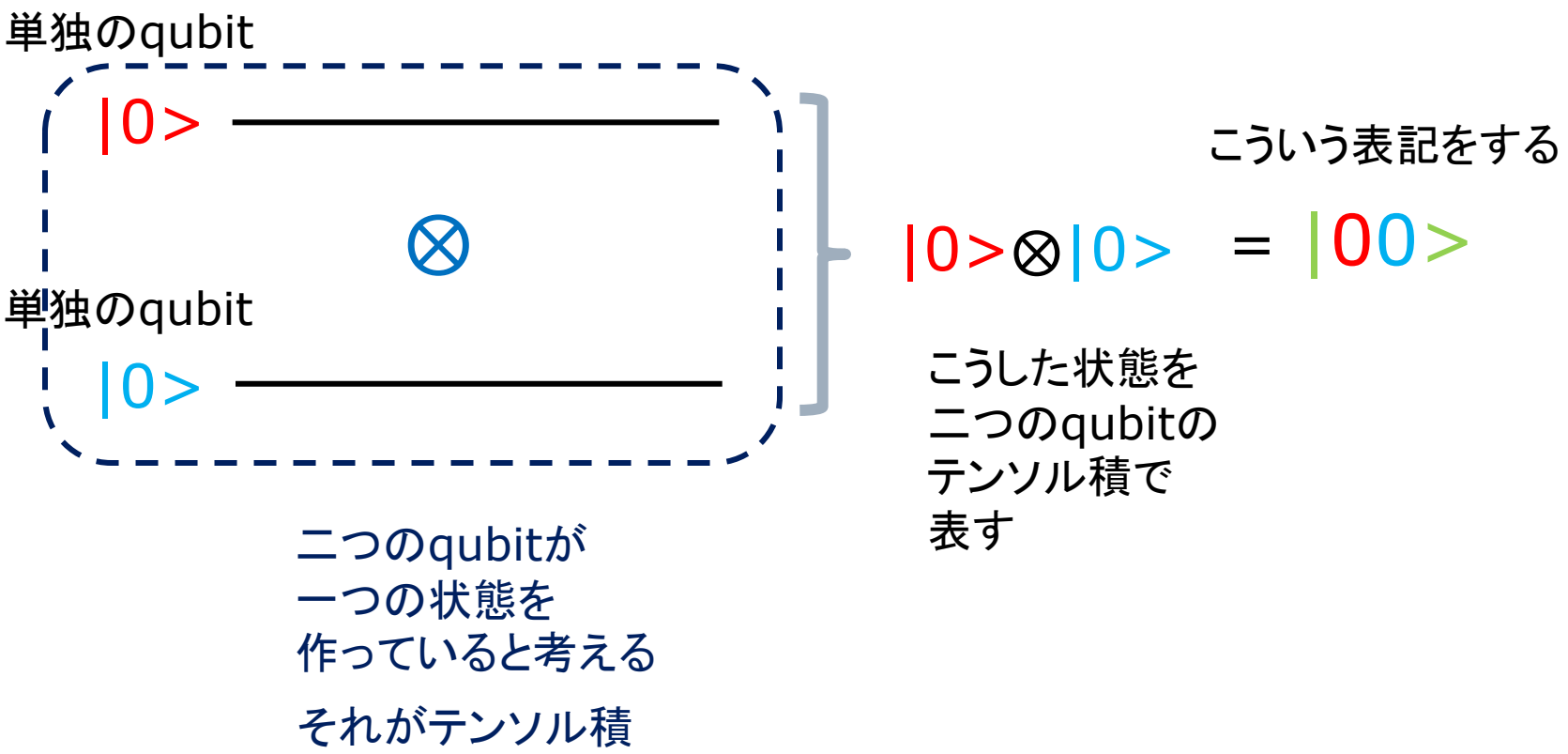
独立した複数のqubitの状態を
一つの状態と考える

2つのqubitのテンソル積

状態S1をとるqubitと
状態S2をとるqubitがあるとしよう。
この時、この二つのqubit 二つを一緒に考えた
状態Sをテンソル積 S1 ⊗ S2で表す。



2つのqubits |0>のテンソル積の例 1



n個の|0> のテンソル積は、
ケットの中身が伸びてゆく

$$|0\rangle \otimes |0\rangle = |00\rangle$$

2つの|0>のテンソル積　　0が2つ

$$|0\rangle \otimes |0\rangle \otimes |0\rangle = |000\rangle$$

3つの|0>のテンソル積　　0が3つ

$$|0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle = |0000\rangle$$

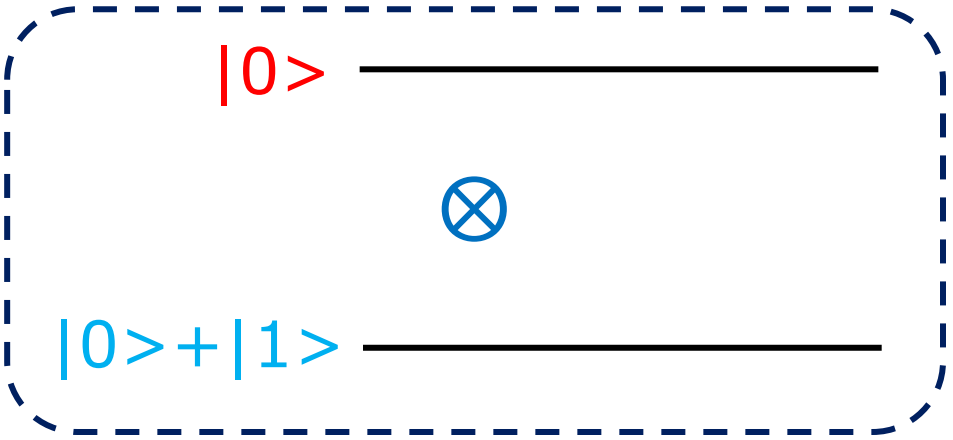
4つの|0>のテンソル積　　0が4つ

$$|0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle = |00000\rangle$$

5つの|0>のテンソル積　　0が5つ

2-qubitsのテンソル積の計算例 2

二つのqubitが
一つの状態を
作っていると考える



こうした状態を
二つのqubitの
テンソル積で
表す

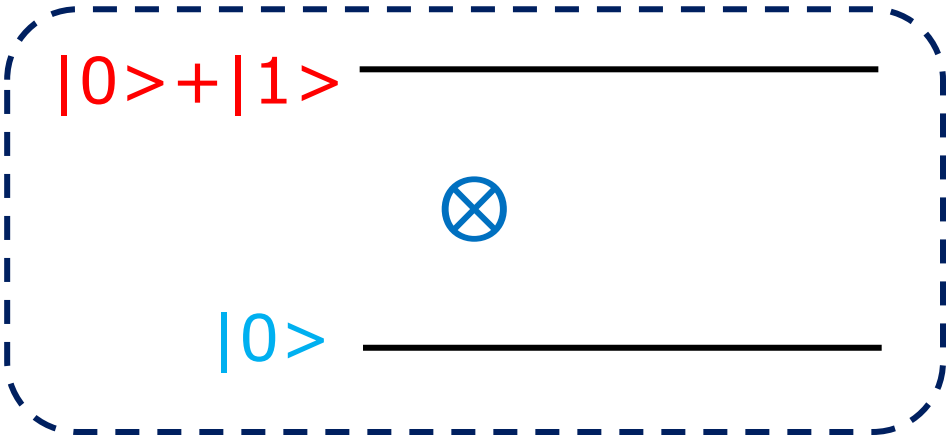
$|0\rangle \otimes (|0\rangle + |1\rangle)$

$|0\rangle \otimes (|0\rangle + |1\rangle) =$
$|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle = |00\rangle + |01\rangle$

$|0\rangle + |1\rangle$という形は本当はおかしい。$\alpha|0\rangle + \beta|1\rangle$の時、$|\alpha|^2 + |\beta|^2 = 1$ という条件があるからだ。本当は、$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$なのだが、計算では無視している。

2-qubitsのテンソル積の計算例 3

二つのqubitが
一つの状態を
作っていると考える



こうした状態を
二つのqubitの
テンソル積で
表す

$(|0\rangle+|1\rangle)\otimes|0\rangle$

$(|0\rangle+|1\rangle)\otimes|0\rangle = |0\rangle\otimes|0\rangle + |1\rangle\otimes|0\rangle = |00\rangle+|10\rangle$

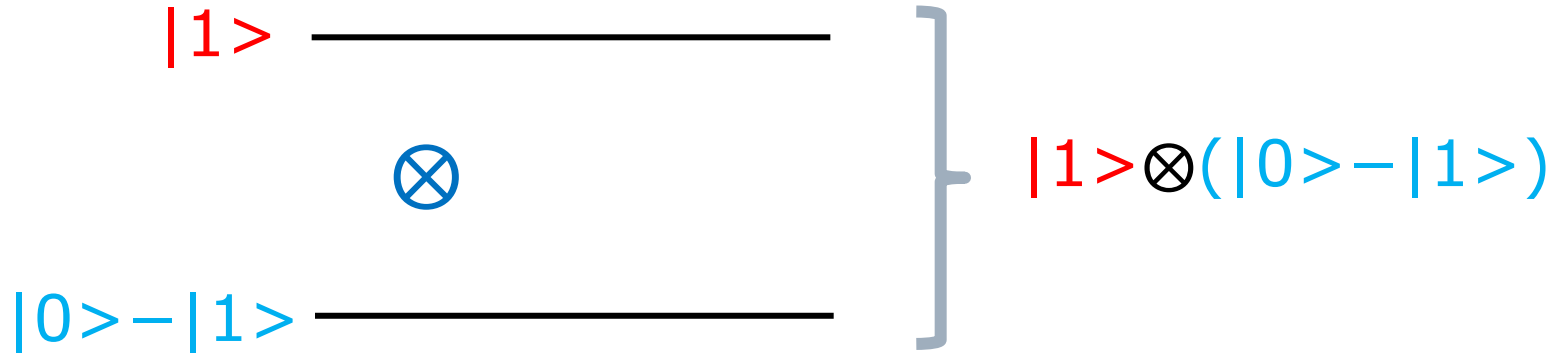
単独のqubit
として見れば、
例2と例3の
qubitは同じ
ものだが、
テンソル積の値は、
積の順序で変わる。

qubitのテンソル積では、積の順序が重要

$$|0\rangle \otimes |1\rangle = |01\rangle$$
$$|1\rangle \otimes |0\rangle = |10\rangle$$

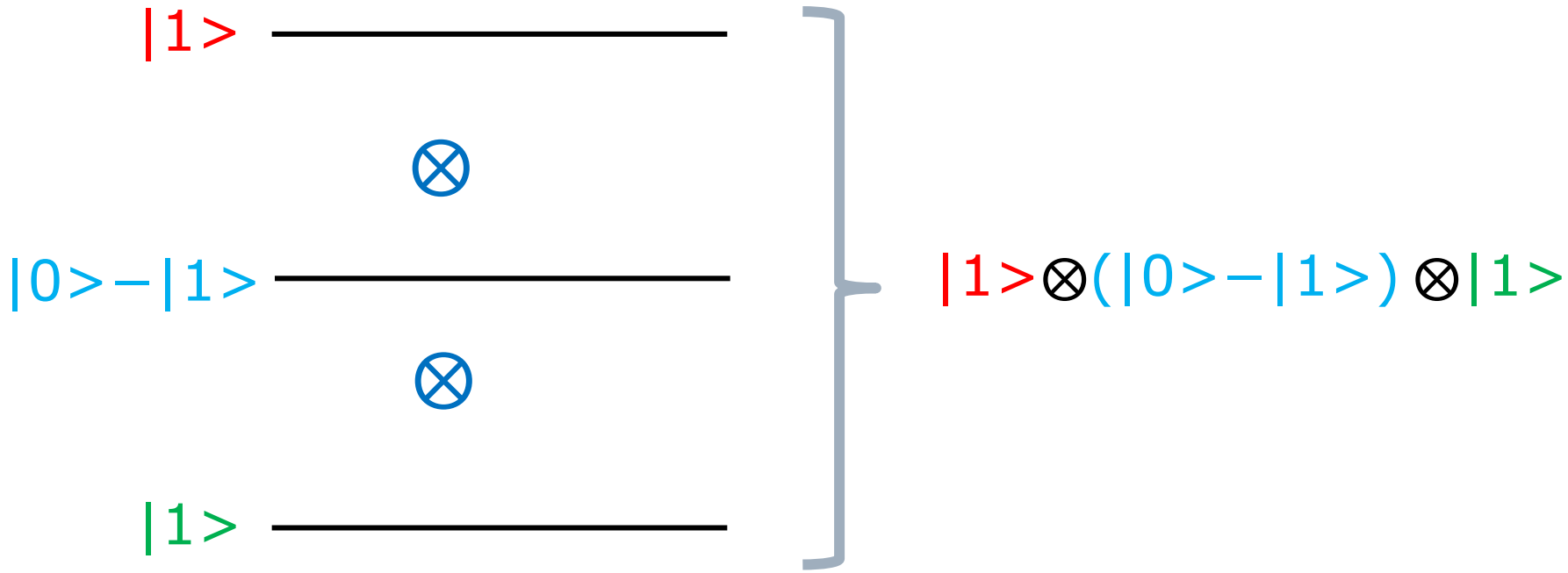
$$|0\rangle \otimes |0\rangle \otimes |0\rangle = |000\rangle$$
$$|0\rangle \otimes |0\rangle \otimes |1\rangle = |001\rangle$$
$$|0\rangle \otimes |1\rangle \otimes |0\rangle = |010\rangle$$
$$|0\rangle \otimes |1\rangle \otimes |1\rangle = |011\rangle$$
$$|1\rangle \otimes |0\rangle \otimes |0\rangle = |100\rangle$$
$$|1\rangle \otimes |0\rangle \otimes |1\rangle = |101\rangle$$
$$|1\rangle \otimes |1\rangle \otimes |0\rangle = |110\rangle$$
$$|1\rangle \otimes |1\rangle \otimes |1\rangle = |111\rangle$$

2-qubitsのテンソル積の計算例 4



$|1\rangle \otimes (|0\rangle - |1\rangle) =$
$|1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle = |10\rangle - |11\rangle$

3-qubitsのテンソル積の計算例 5



$$
\begin{aligned}
&|1\rangle \otimes (|0\rangle - |1\rangle) \otimes |1\rangle \\
&= (|1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \otimes |1\rangle \\
&= (|10\rangle - |11\rangle) \otimes |1\rangle = |101\rangle - |111\rangle
\end{aligned}
$$

3-qubitsのテンソル積の計算例 6

$|\psi> = \alpha|0> + \beta|1>$, $|\Phi^+> = 1/\sqrt{2}\,(|00> + |11>)$
として、$|\psi_0> = |\psi> \otimes |\Phi^+>$ を求めよ。

$$|\psi_0> = |\psi> \otimes |\Phi^+>$$

$$= (\alpha|0> + \beta|1>) \otimes 1/\sqrt{2}\,(|00> + |11>)$$

$$= 1/\sqrt{2}\,(\alpha|0> \otimes (|00> + |11>) + \beta|1> \otimes (|00> + |11>))$$

3-qubitsのテンソル積の計算例 7

$$1/\sqrt{2}\,(\alpha(|0>+|1>)\otimes(|00>+|11>)+$$
$$\beta(|0>-|1>)\otimes(|10>+|01>)\,)$$

$$=1/\sqrt{2}\,(\alpha(|000>+|011>+|100>+|111>)+$$
$$\beta(|010>+|001>-|110>-|101>)\,)$$

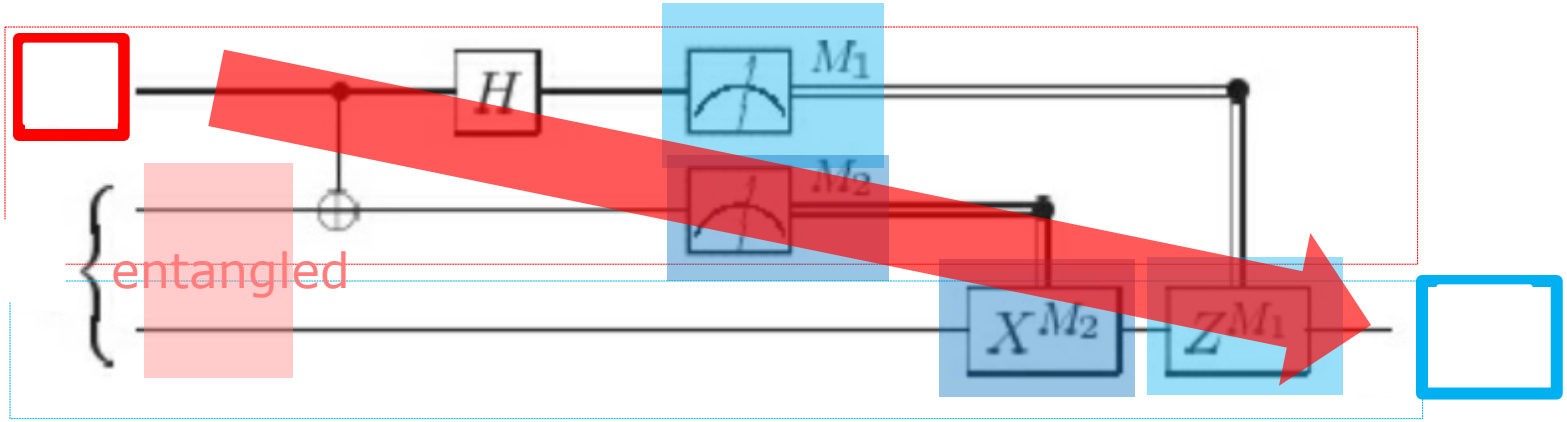
$$=1/\sqrt{2}\,(|00>(\alpha|0>+\beta|1>)+$$
$$|01>(\alpha|1>+\beta|0>)+$$
$$|10>(\alpha|0>-\beta|1>)+$$
$$|11>\,(\alpha|1>-\beta|0>)\,)$$

量子テレポーテーション

-- 量子テレポーテーションを計算する --

量子テレポーテーション回路の動き

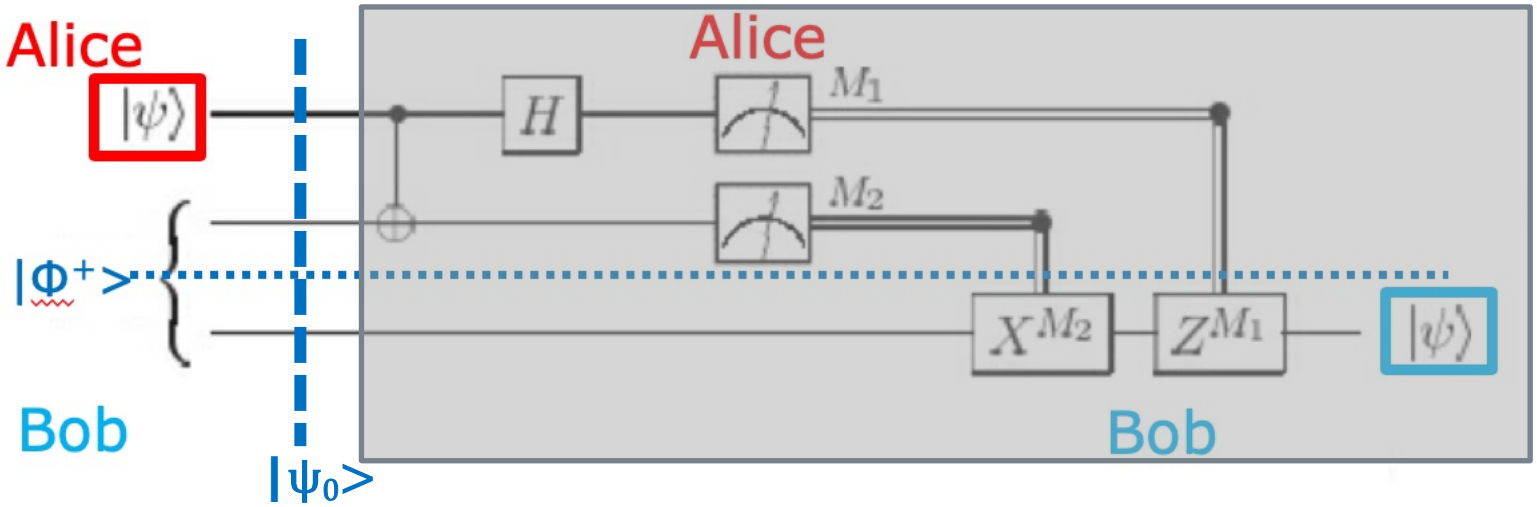
Alice



Bob

AliceとBobはエンタングルしている。
Aliceは第一レジスターにqubit $|\psi>$ を置く。
Aliceは、第一レジスターを観測して、Zゲートをコントロールする。
Aliceは、第二レジスターを観測して、Xゲートをコントロールする。
Aliceのqubit $|\psi>$の情報は、Bob側に転送される。

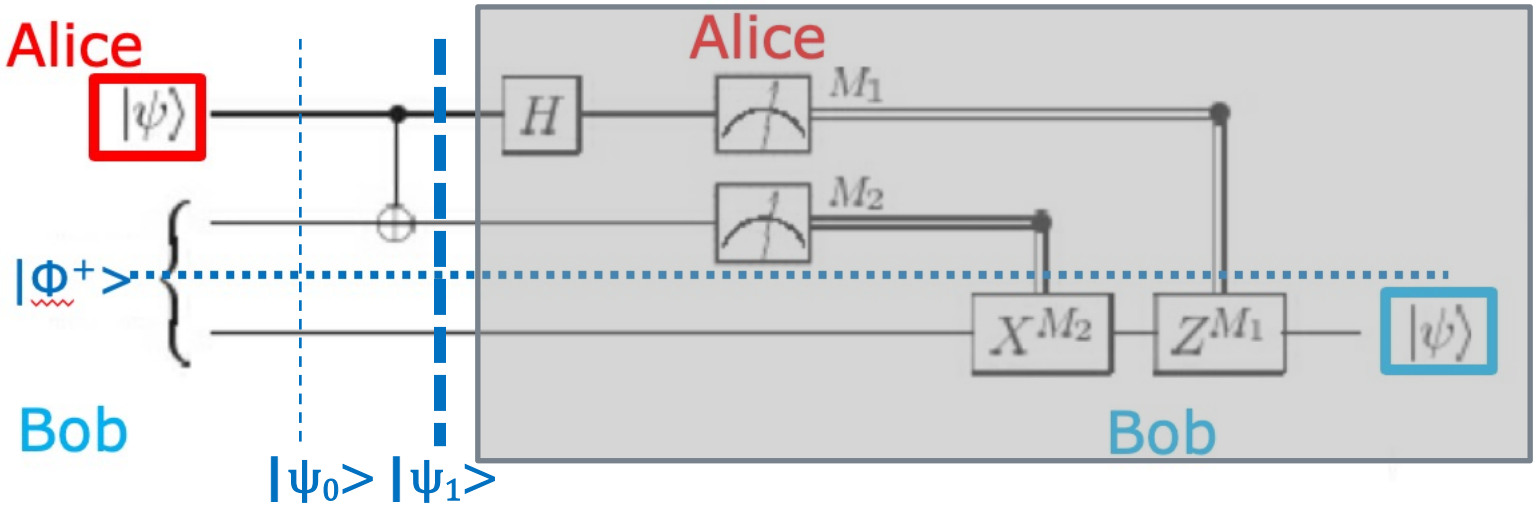
量子テレポーテーションを計算する



$|\psi\rangle = \alpha|0\rangle+\beta|1\rangle$, $|\Phi^+\rangle = 1/\sqrt{2}\,(|00\rangle + |11\rangle)$ とすると。

$$|\psi_0\rangle = |\psi\rangle \otimes |\Phi^+\rangle$$
$$= (\alpha|0\rangle+\beta|1\rangle) \otimes 1/\sqrt{2}\,(|00\rangle + |11\rangle)$$
$$= 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle +|11\rangle)+\beta|1\rangle\otimes(|00\rangle + |11\rangle))$$

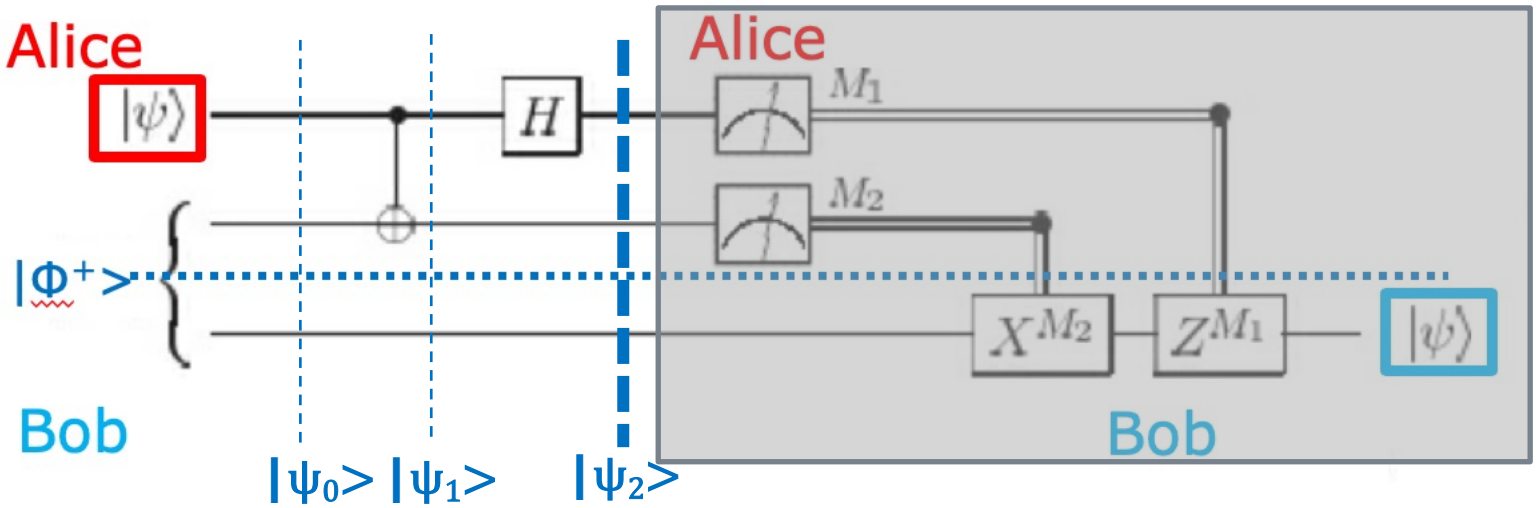
回路に入る直前の段階でのシステムの状態を$|\psi_0\rangle$とする



$$|\psi_0\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle)+\beta|1\rangle\otimes(|00\rangle + |11\rangle))$$

$$|\psi_1\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle)+\beta|1\rangle\otimes(|10\rangle + |01\rangle))$$

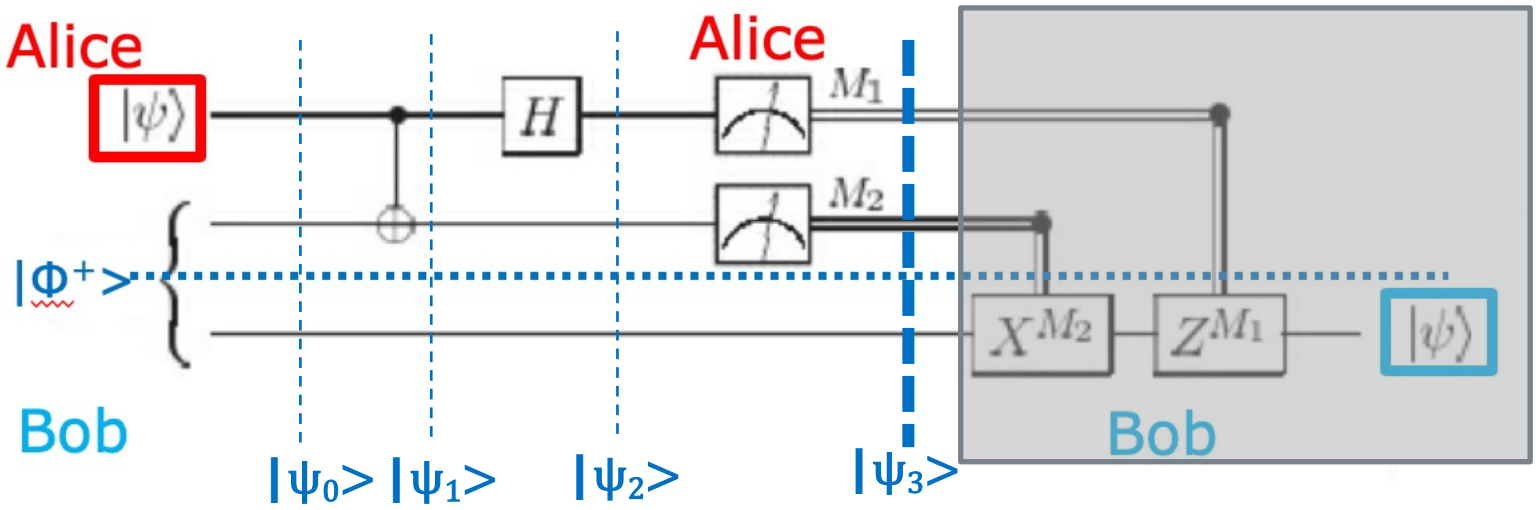
回路上のCNOTを実行した直後の $|\psi_1\rangle$段階でのシステムの状態



$$|\psi_0\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|00\rangle + |11\rangle))$$

$$|\psi_1\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|10\rangle + |01\rangle))$$

$$\begin{aligned}|\psi_2\rangle &= 1/\sqrt{2}\,(\alpha(|0\rangle+|1\rangle)\otimes(|00\rangle + |11\rangle) + \\ &\qquad \beta(|0\rangle-|1\rangle)\otimes(|10\rangle + |01\rangle)\,) \\ &= 1/\sqrt{2}\,(\alpha(|000\rangle+|011\rangle+|100\rangle+|111\rangle) + \\ &\qquad \beta(|010\rangle+|001\rangle-|110\rangle-|101)\,) \\ &= 1/\sqrt{2}\,(|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle) + \\ &\qquad |10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle\,(\alpha|1\rangle-\beta|0\rangle)\,)\end{aligned}$$

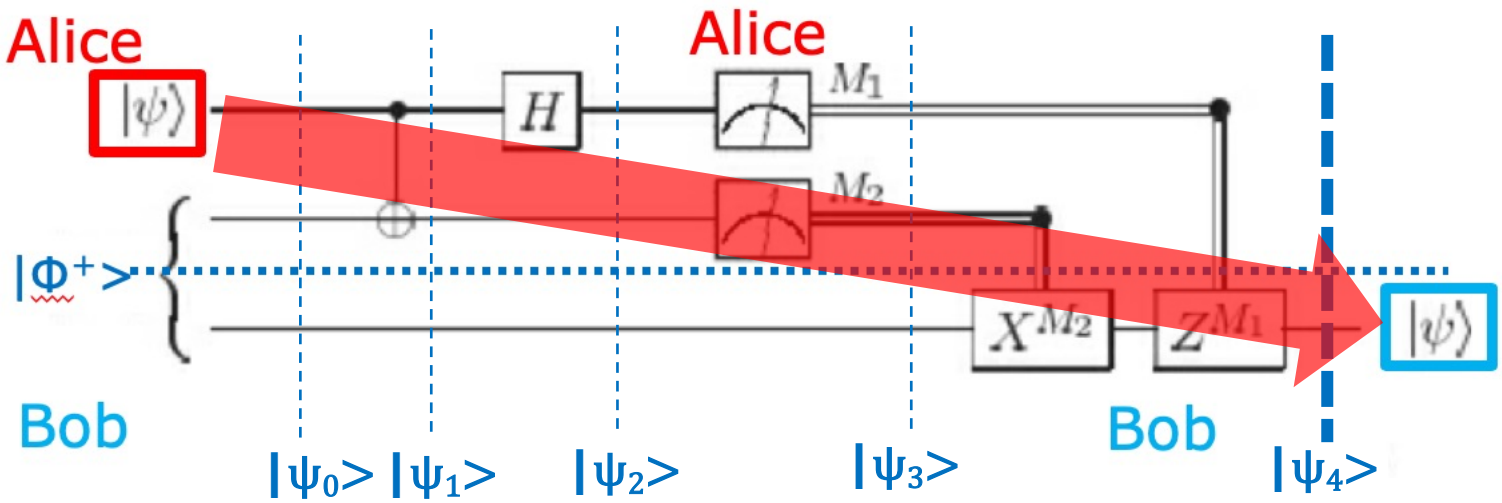


$$|\psi_0\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|00\rangle + |11\rangle))$$

$$|\psi_1\rangle = 1/\sqrt{2}\,(\alpha|0\rangle \otimes(|00\rangle + |11\rangle) + \beta|1\rangle \otimes(|10\rangle + |01\rangle))$$

$$|\psi_2\rangle = 1/\sqrt{2}\,(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle\,(\alpha|1\rangle - \beta|0\rangle)\,)$$

$$|\psi_3(00)\rangle = (\alpha|0\rangle + \beta|1\rangle)$$
$$|\psi_3(01)\rangle = (\alpha|1\rangle + \beta|0\rangle)$$
$$|\psi_3(10)\rangle = (\alpha|0\rangle - \beta|1\rangle)$$
$$|\psi_3(11)\rangle = (\alpha|1\rangle - \beta|0\rangle)$$



$|\psi_3(00)\rangle = (\alpha|0\rangle+\beta|1\rangle)$
$|\psi_3(01)\rangle = (\alpha|1\rangle+\beta|0\rangle)$
$|\psi_3(10)\rangle = (\alpha|0\rangle-\beta|1\rangle)$
$|\psi_3(11)\rangle = (\alpha|1\rangle-\beta|0\rangle)$

$|\psi_4(00)\rangle = \psi_3(00)\rangle = (\alpha|0\rangle+\beta|1\rangle)$
$|\psi_4(01)\rangle = X\,|\psi_3(01)\rangle = X(\alpha|1\rangle+\beta|0\rangle) = (\alpha|0\rangle+\beta|1\rangle)$
$|\psi_4(10)\rangle = Z|\psi_3(10)\rangle = Z(\alpha|0\rangle-\beta|1\rangle) = (\alpha|0\rangle+\beta|1\rangle)$
$|\psi_4(11)\rangle = ZX|\psi_3(11)\rangle = ZX\,(\alpha|1\rangle-\beta|0\rangle) = (\alpha|0\rangle+\beta|1\rangle)$

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

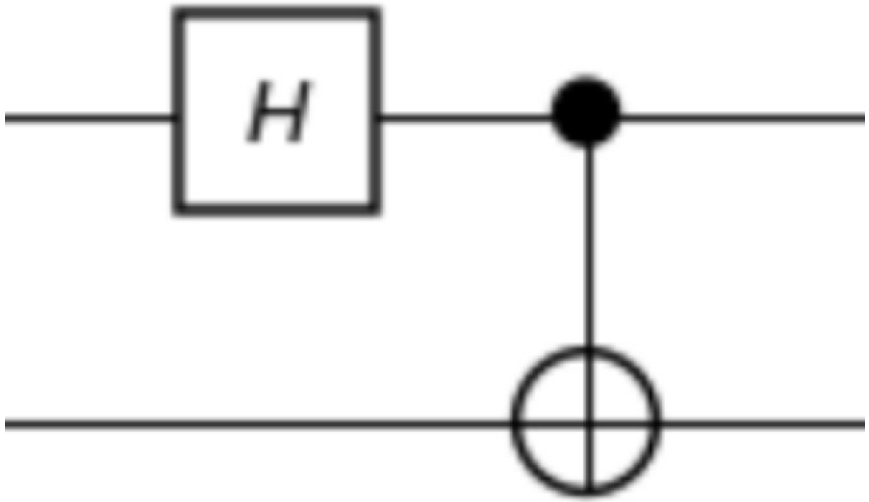
Aliceのqubit $|\psi\rangle$の情報は、Bob側に転送された！

量子テレポーテーション

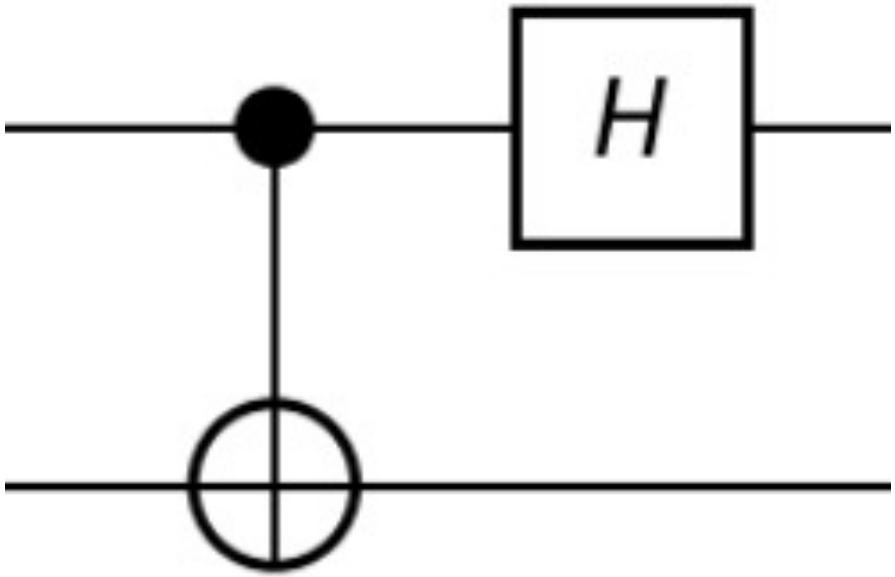
-- Bell State Gate と Bell Measure Gate --

Bell State Gateと
Bell Measure Gate

Bell State Gate

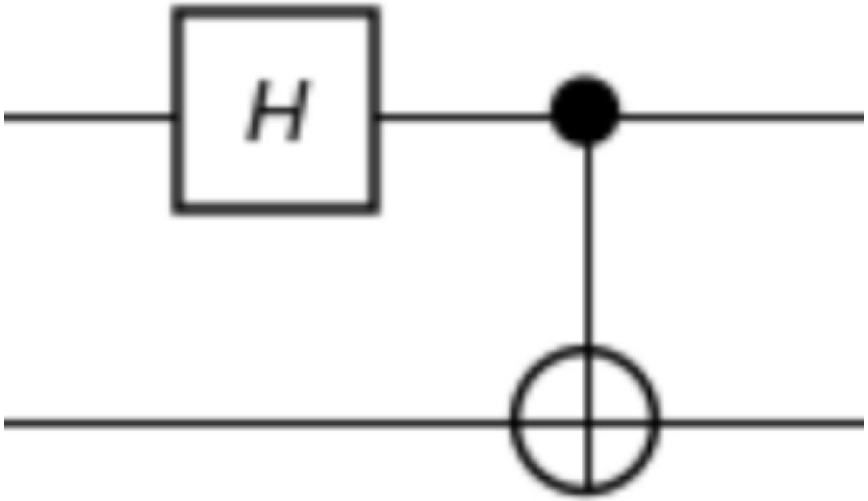


Bell Measure Gate

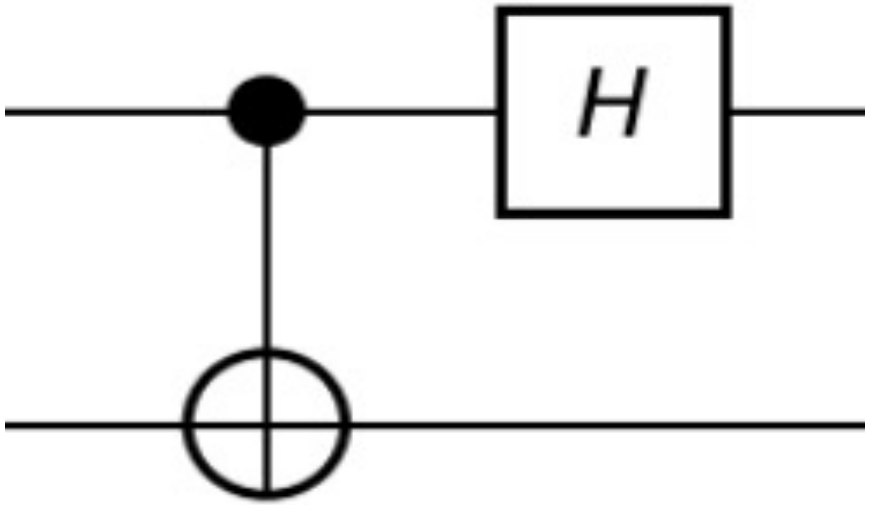


Bell State Gateと
Bell Measure Gate

Bell State Gate

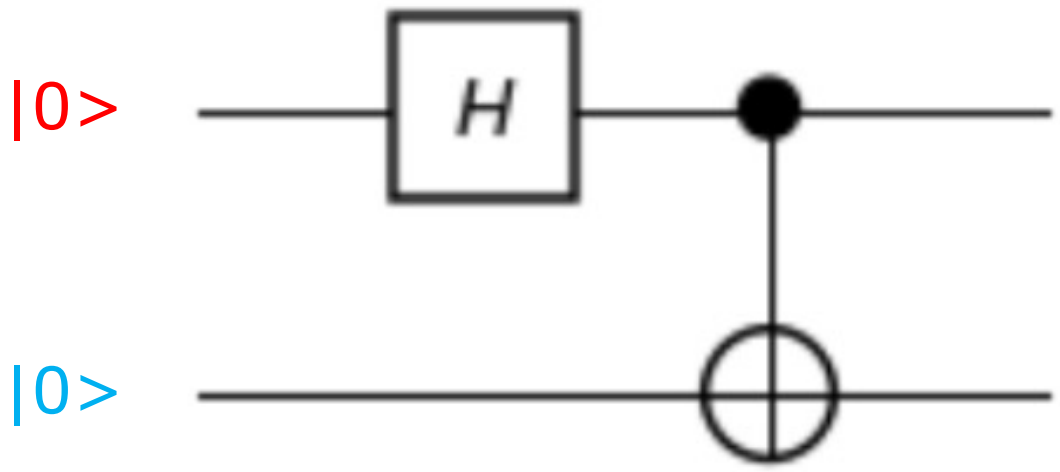


Bell Measure Gate



Bell State Gateの働き

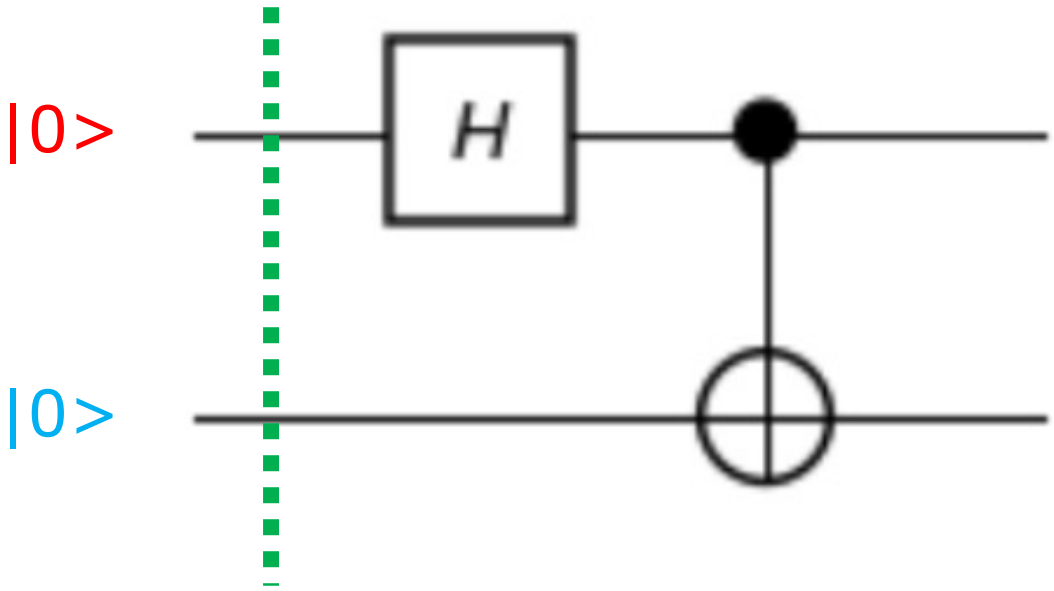
Bell State ゲートの働き
入力|00>の場合



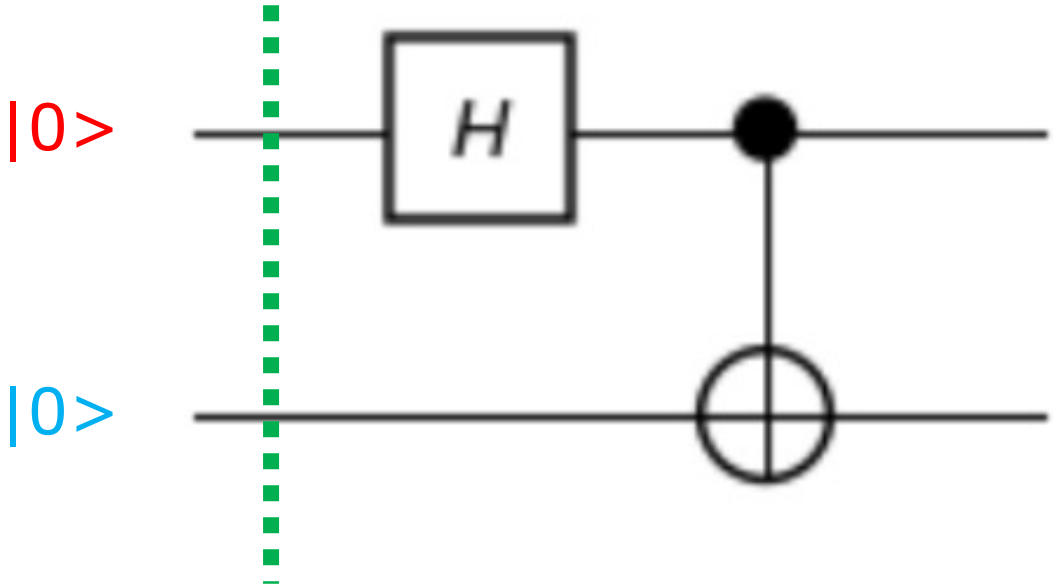
Bell State ゲートの働き

入力|00>の場合

この時点での
系全体の状態
を調べる



Bell State ゲートの働き
入力|00>の場合



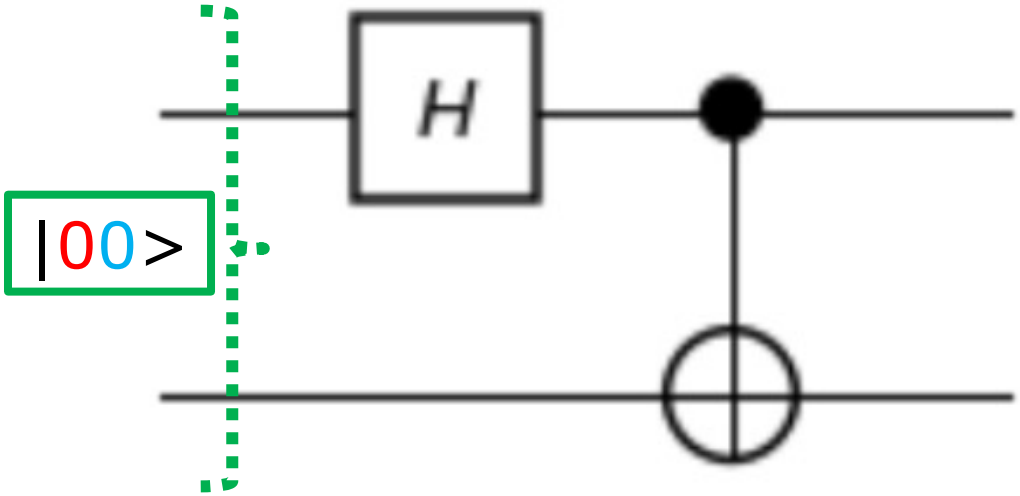
$|0\rangle \otimes |0\rangle$

この時点での
系全体の状態

$= \boxed{|00\rangle}$

Bell State ゲートの働き

入力|00>の場合

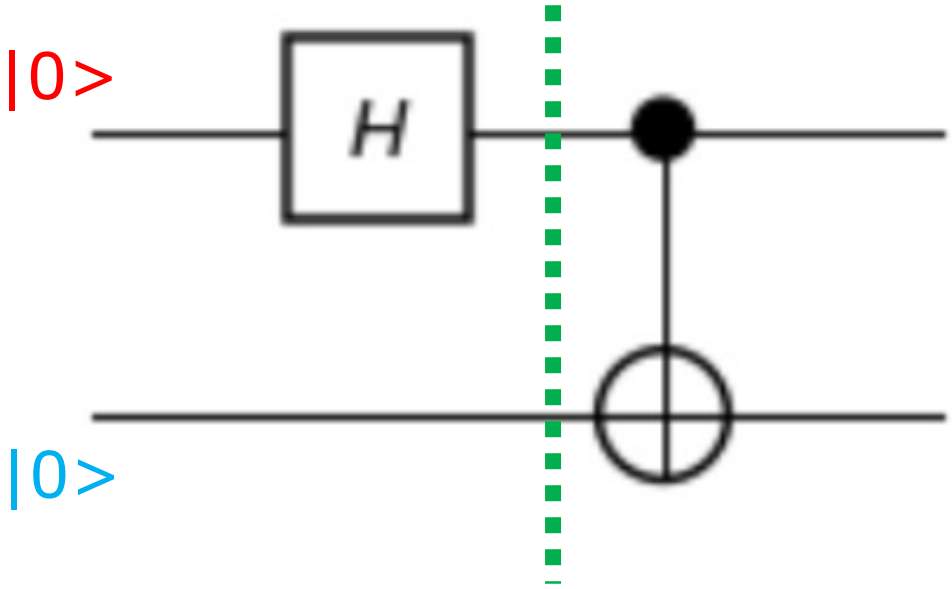


分離可能

Bell State ゲートの働き

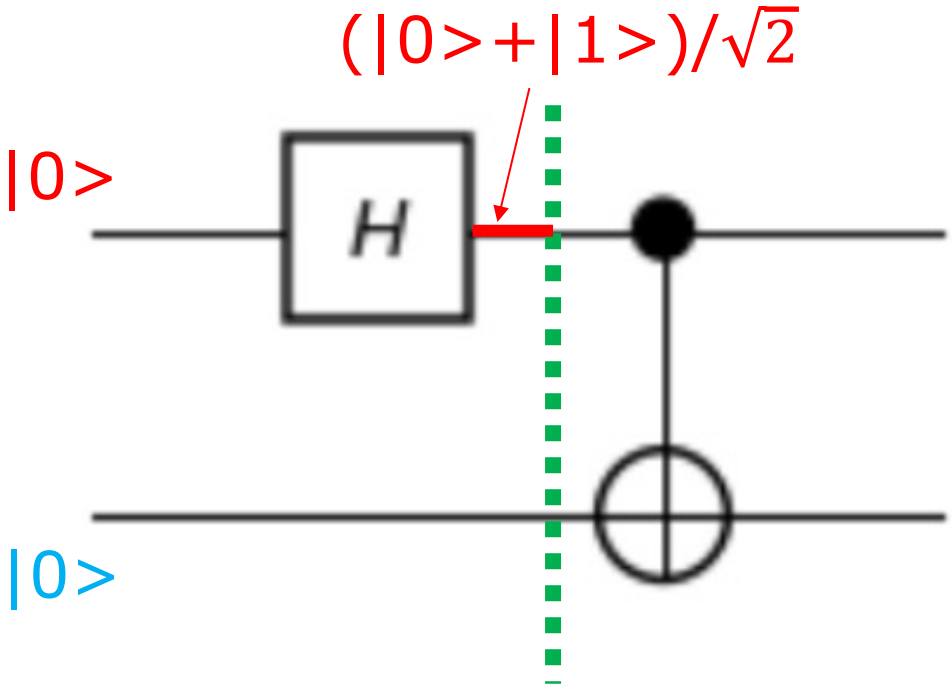
入力|00>の場合

この時点での
系全体の状態
を調べる



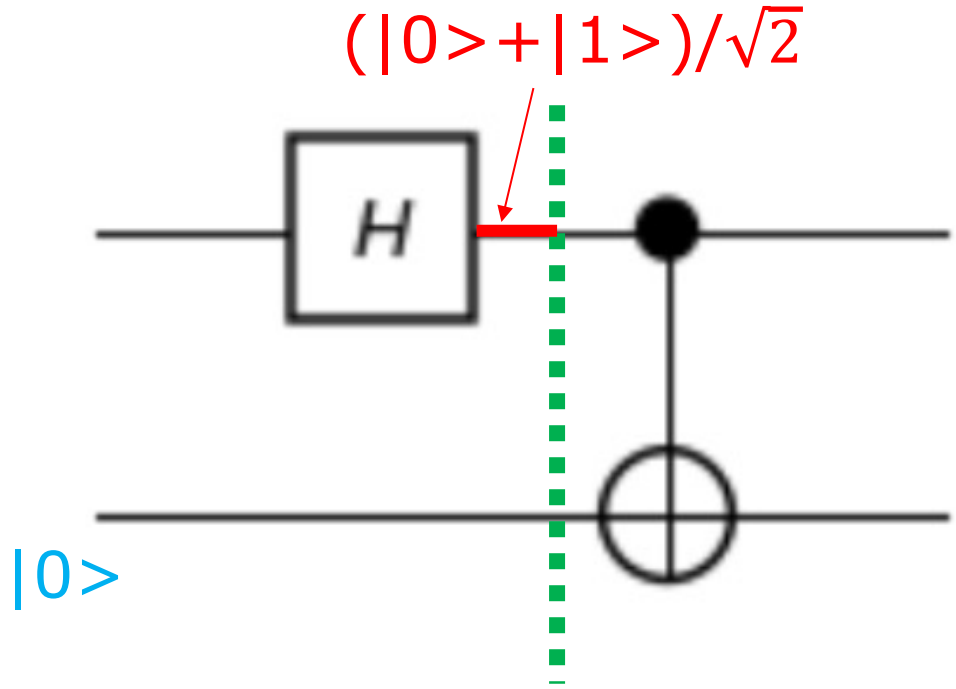
Bell State ゲートの働き

入力|00>の場合



Hは|0>を
(|0>+|1>)/√2に
変える

Bell State ゲートの働き
入力|00>の場合

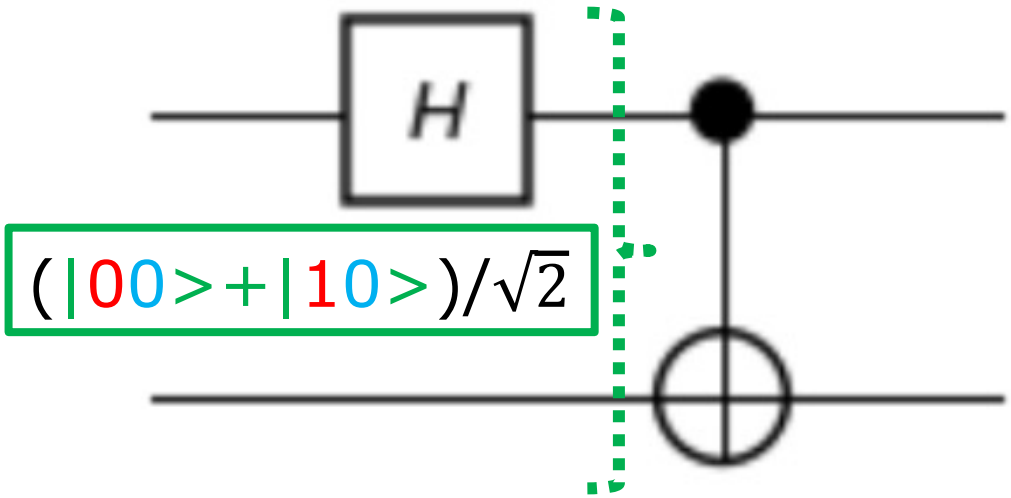


この時点での
系全体の状態

$= (|00\rangle + |10\rangle)/\sqrt{2}$

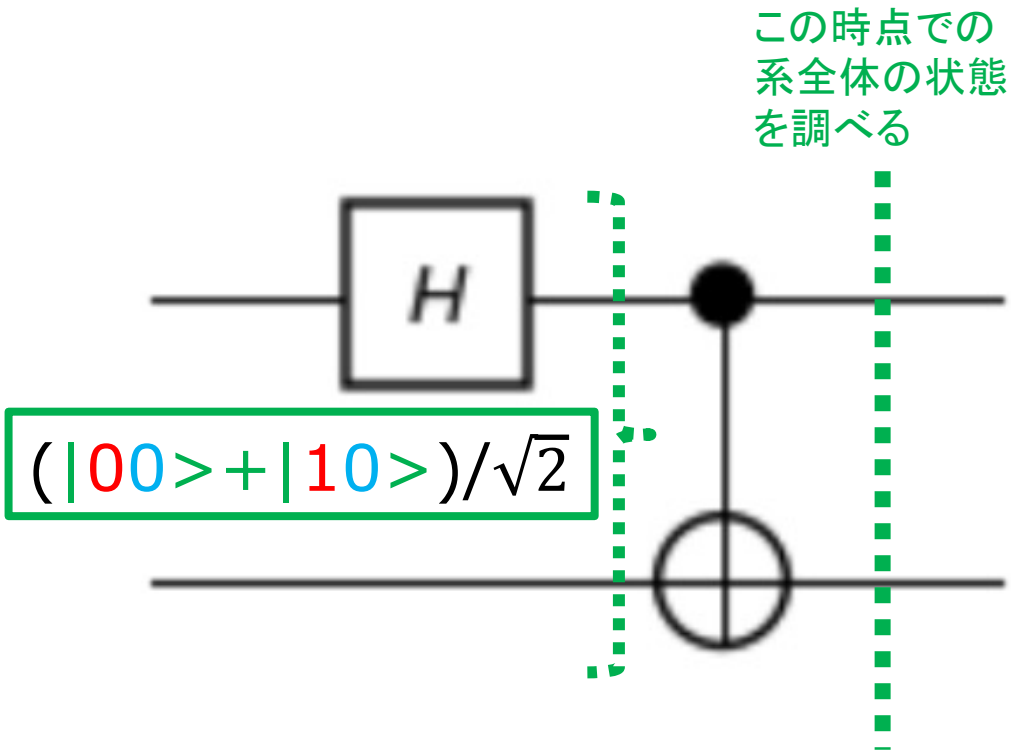
Bell State ゲートの働き

入力|00>の場合

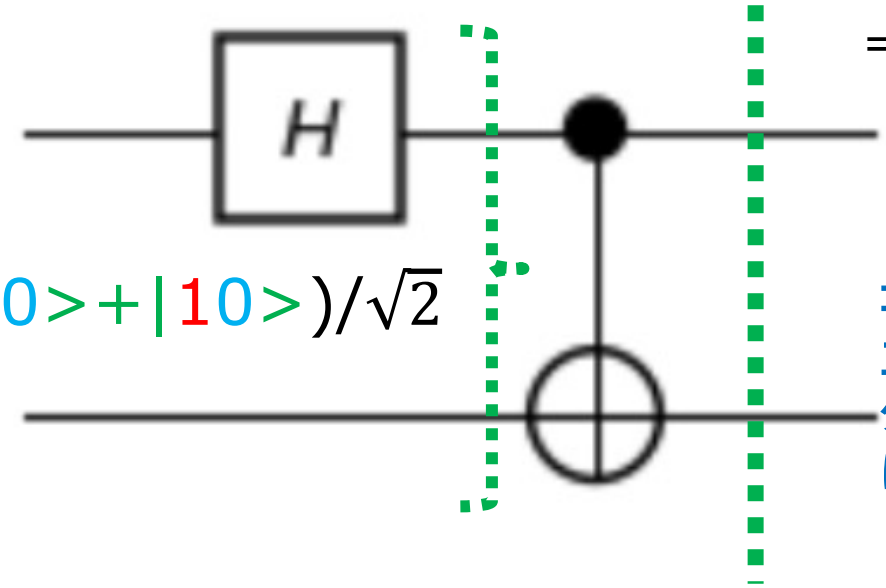


Bell State ゲートの働き

入力|00>の場合



Bell State ゲートの働き
入力|00>の場合



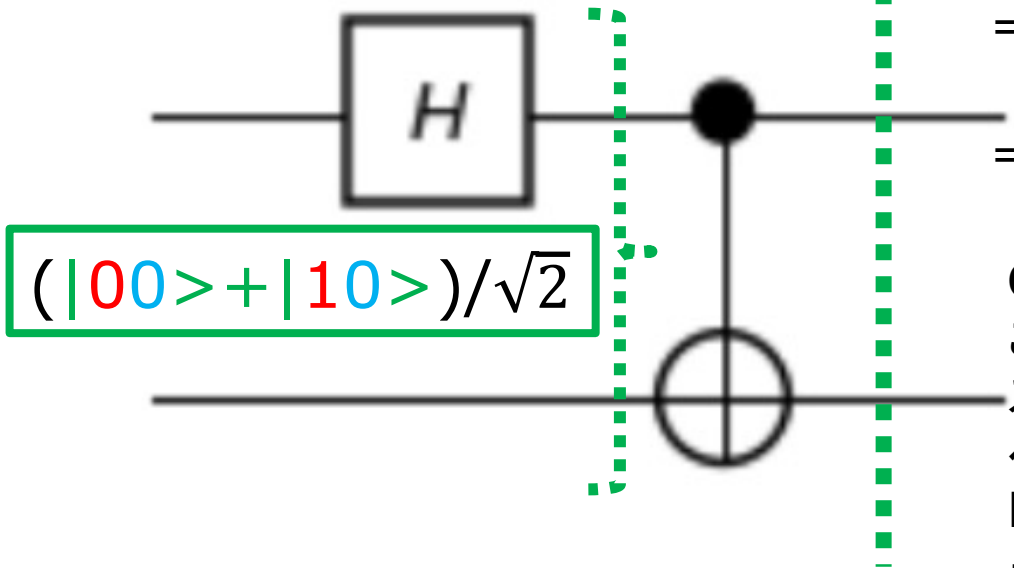
$(|00\rangle+|10\rangle)/\sqrt{2}$

CNOT$((|00\rangle+|10\rangle)/\sqrt{2})$
$= (|00\rangle+|11\rangle)/\sqrt{2}$

コントロールビットに**1**が
立っている項だけで
ターゲットビットを反転すれ
ばいい

Bell State ゲートの働き

入力|00>の場合

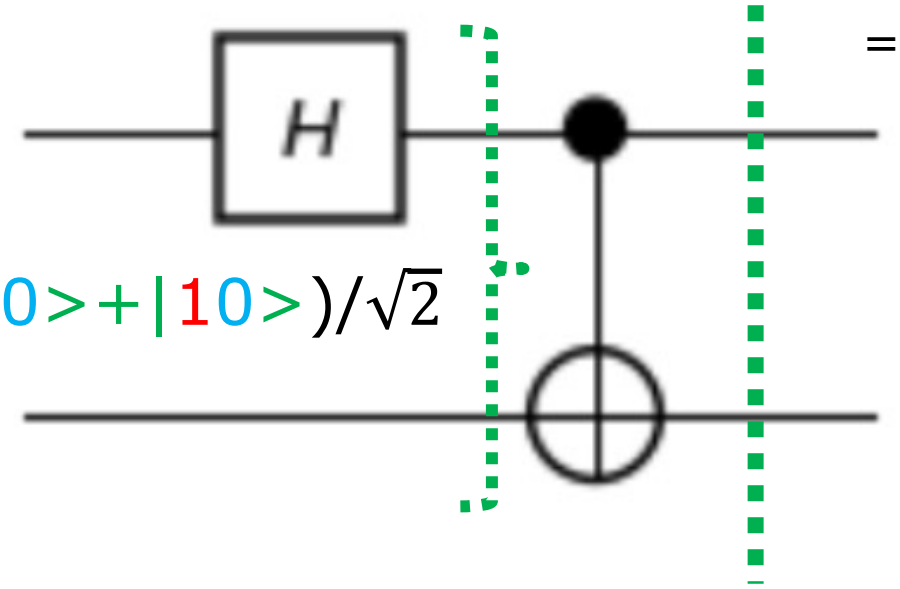


CNOT((|00>+|10>) /√2)
= **CNOT**(|00>) /√2
+**CNOT**(|10>) /√2
= (|00>+|11>) /√2

CNOTは線形演算子である。
ここでは、線形演算子Mで
スカラー a,b
ベクトル u,v について
M(au+bv)
= aM(u)+bM(v)
を利用した。

また、
CNOT(|00>) = |00>
CNOT(|10>) = |11>
である。

Bell State ゲートの働き
入力|00>の場合



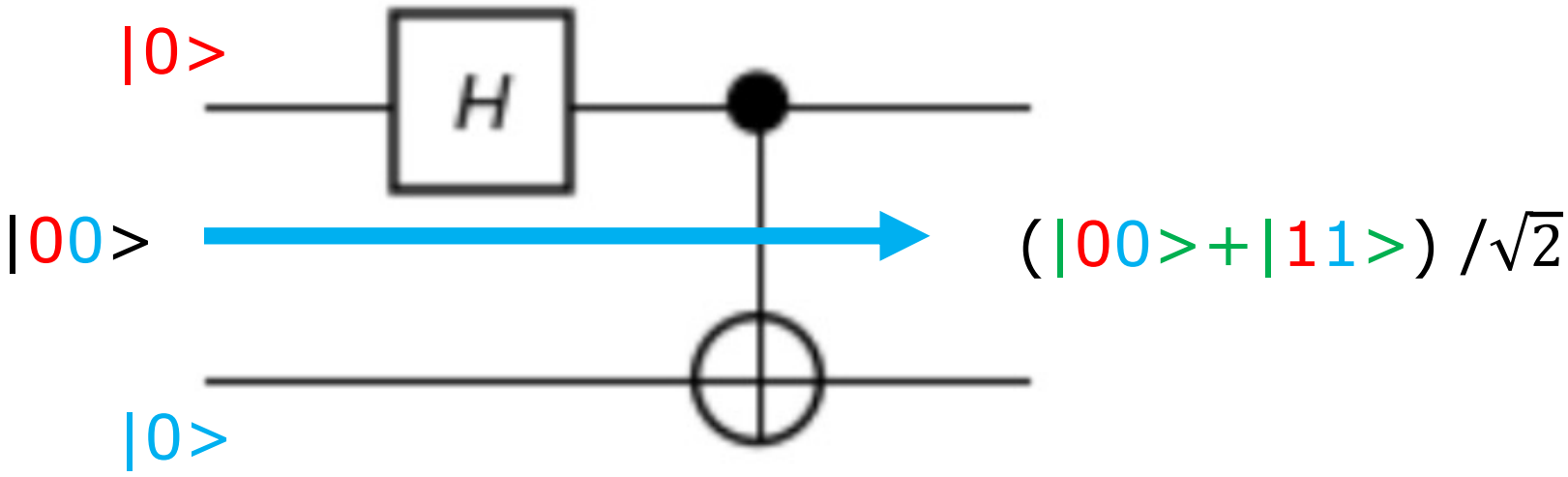
$(|00\rangle+|10\rangle)/\sqrt{2}$

CNOT$((|00\rangle+|10\rangle)/\sqrt{2})$
$= (|00\rangle+|11\rangle)/\sqrt{2}$

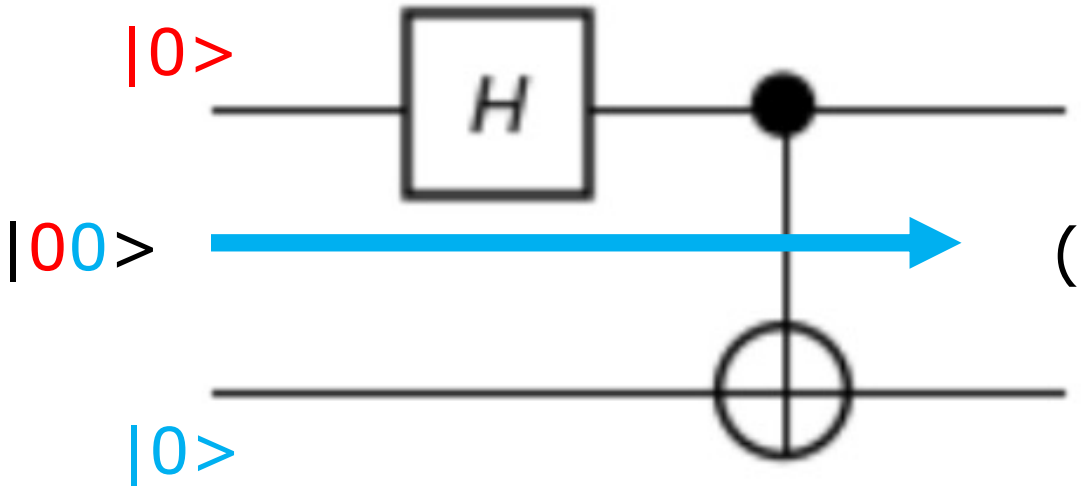
この時点での
系全体の状態

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

Bell State ゲートの働き
入力|00>の場合



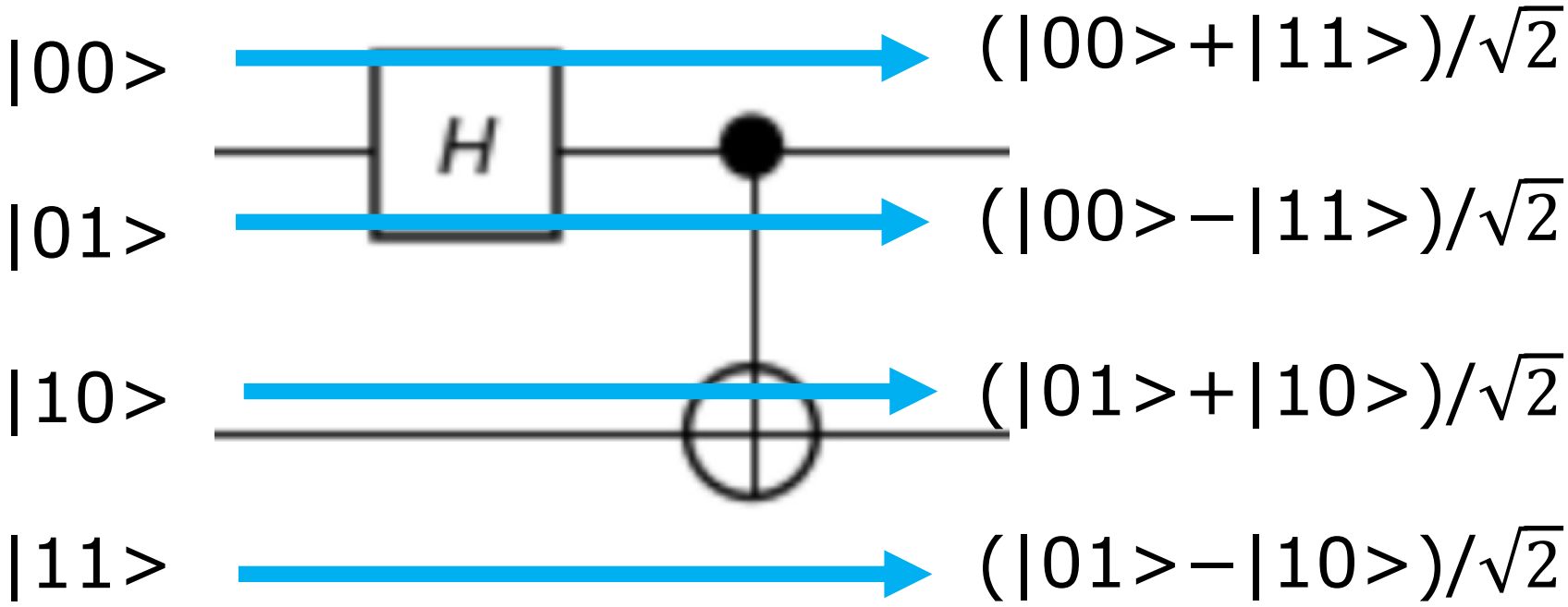
Bell State ゲートの働き
入力|00>の場合



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

これは、エンタングルメント状態の
Bell Stateの一つ$|\Phi^{+}\rangle$である。

Bell State ゲートの働き

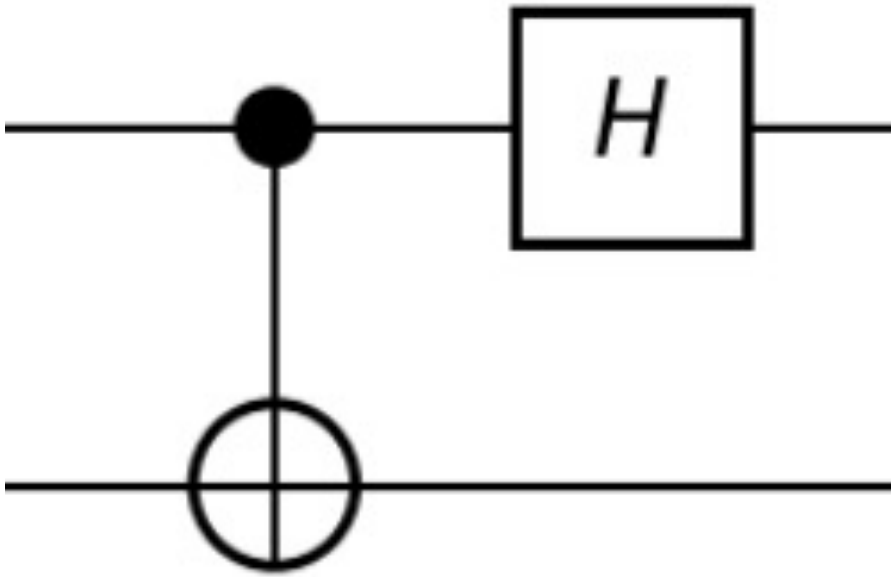


同様の計算で、次のことがわかる。

Bell State ゲートの働き

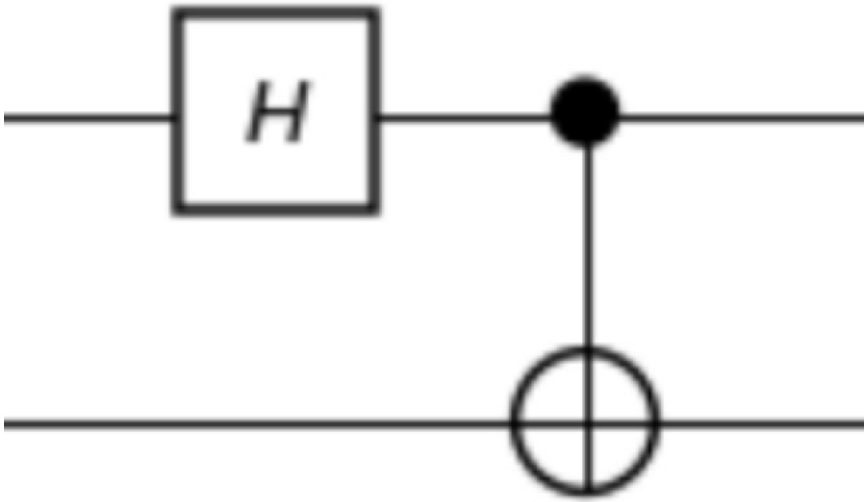
Bell Measure Gateの働き

Bell Measure ゲート

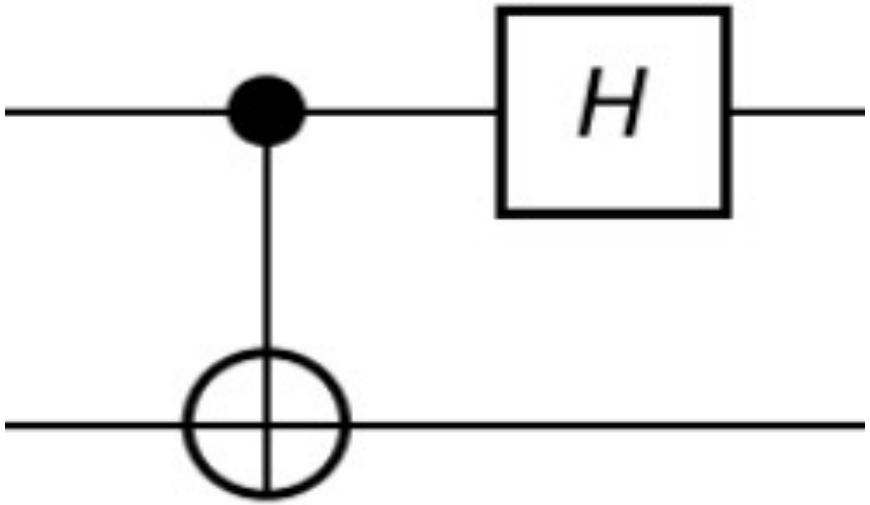


Bell State Gateと
Bell Measure Gate

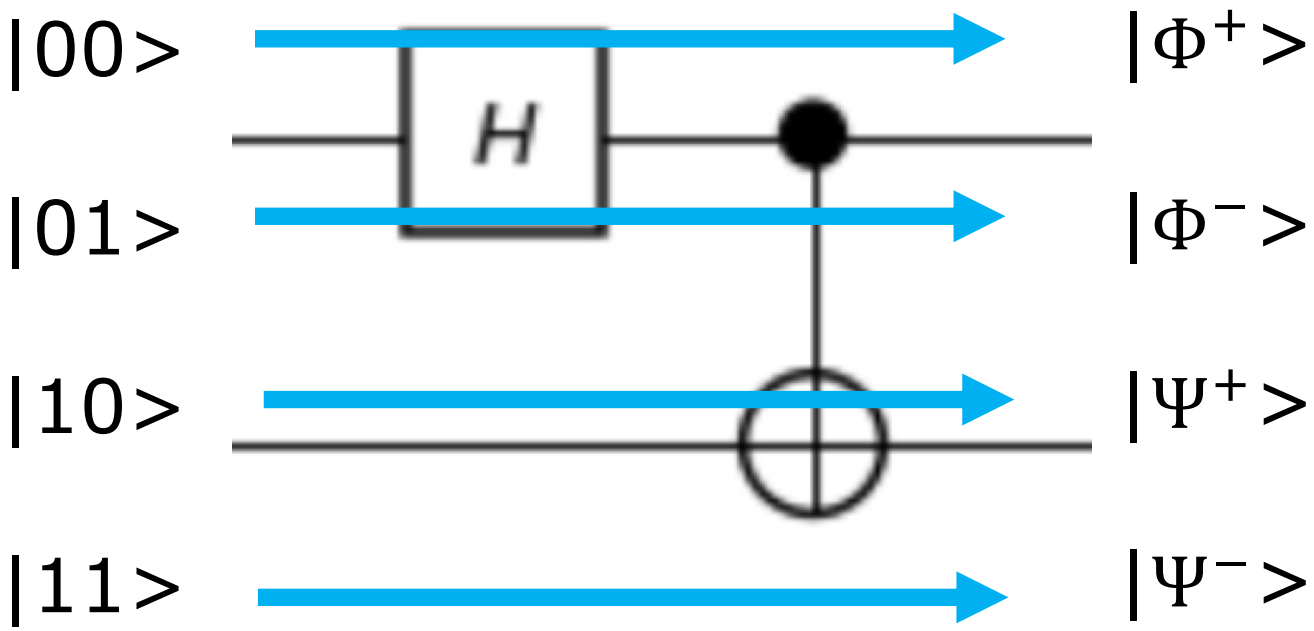
Bell State Gate



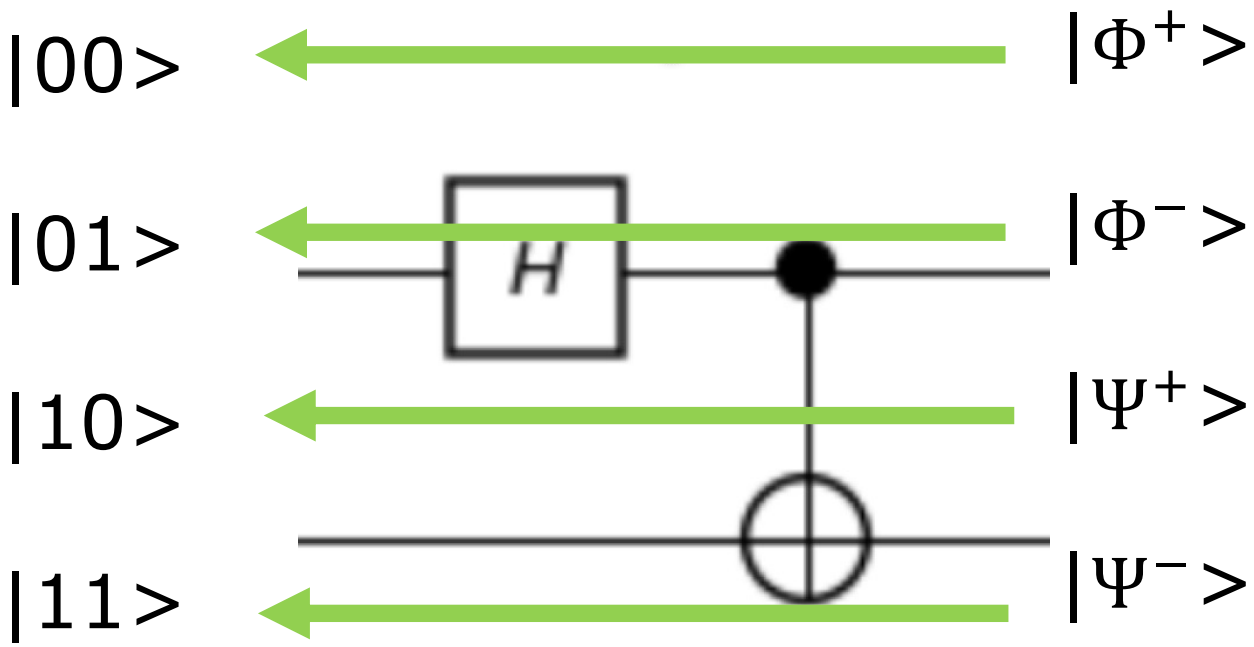
Bell Measure Gate



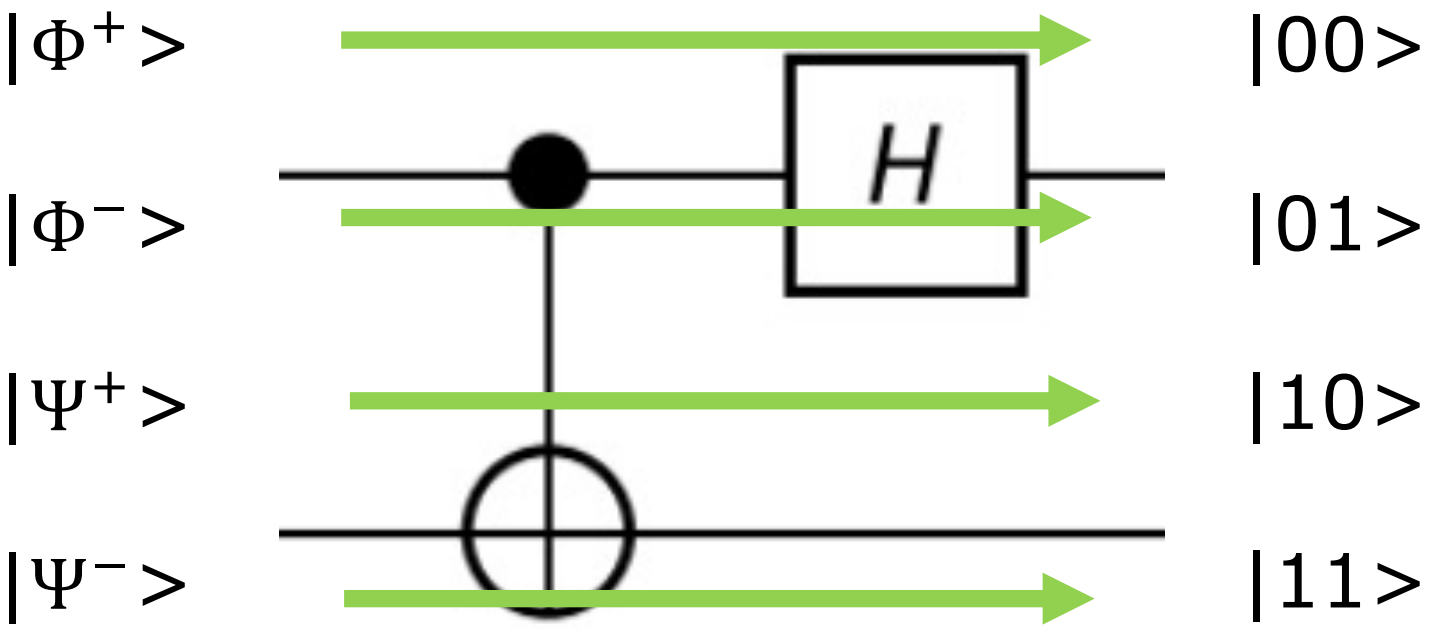
Bell State ゲートの働き



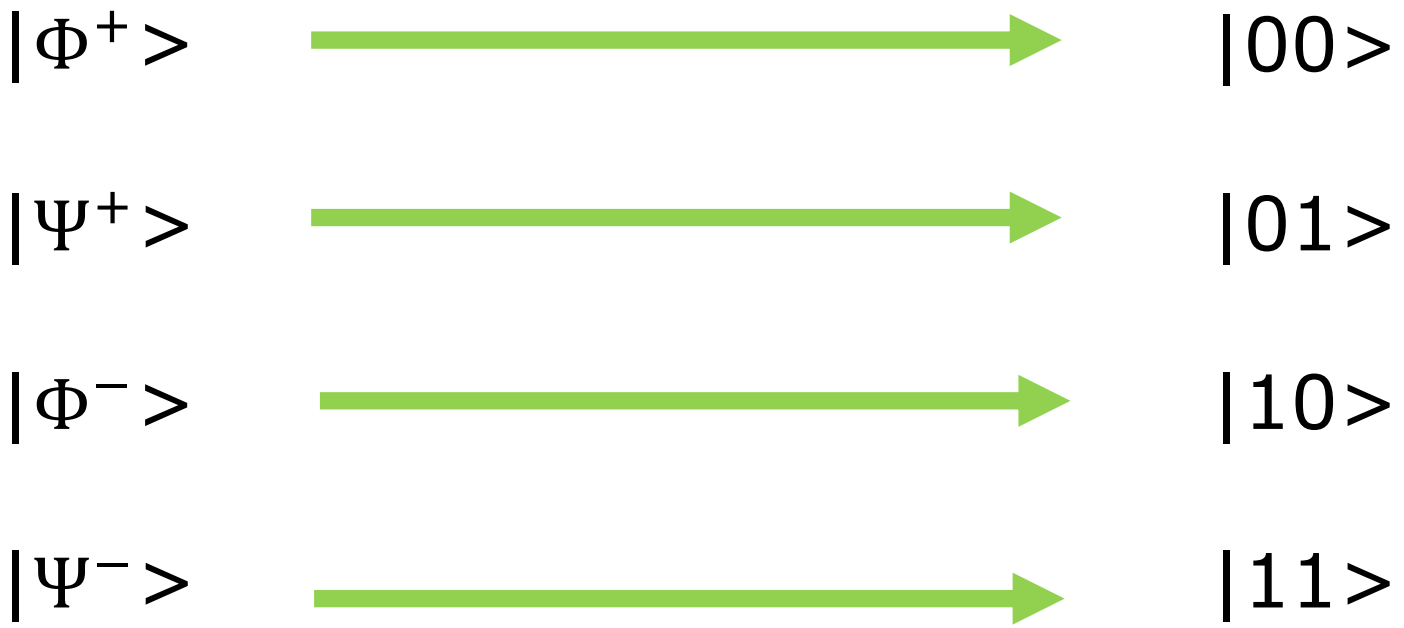
Bell Measure Gate
=(Bell State Gate)$^{-1}$ =(Bell State Gate)†



Bell Measure ゲートの働き



Bell Measure ゲートの働き



Bell 基底と計算基底

Bell 基底

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

$(|00\rangle-|11\rangle)/\sqrt{2} = |\Phi^-\rangle$

$(|01\rangle+|10\rangle)/\sqrt{2} = |\Psi^+\rangle$

$(|01\rangle-|10\rangle)/\sqrt{2} = |\Psi^-\rangle$

として、$|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$
を、Bell 基底と呼ぶ。

Bell 基底と計算基底

この時、次の式が成り立つ。

$$|00\rangle = (|\Phi^+\rangle + |\Phi^-\rangle)\sqrt{2}/2$$

$$|11\rangle = (|\Phi^+\rangle - |\Phi^-\rangle)\sqrt{2}/2$$

$$|01\rangle = (|\Psi^+\rangle + |\Psi^-\rangle)\sqrt{2}/2$$

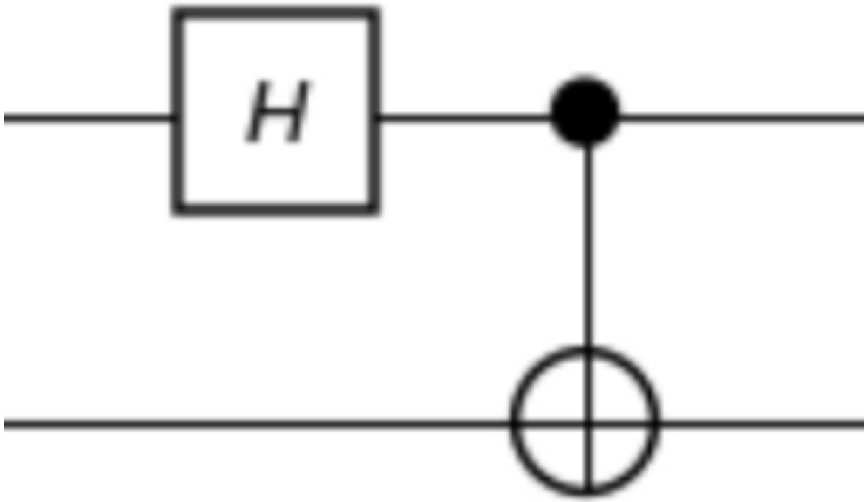
$$|10\rangle = (|\Psi^+\rangle - |\Psi^-\rangle)\sqrt{2}/2$$

量子テレポーテーション

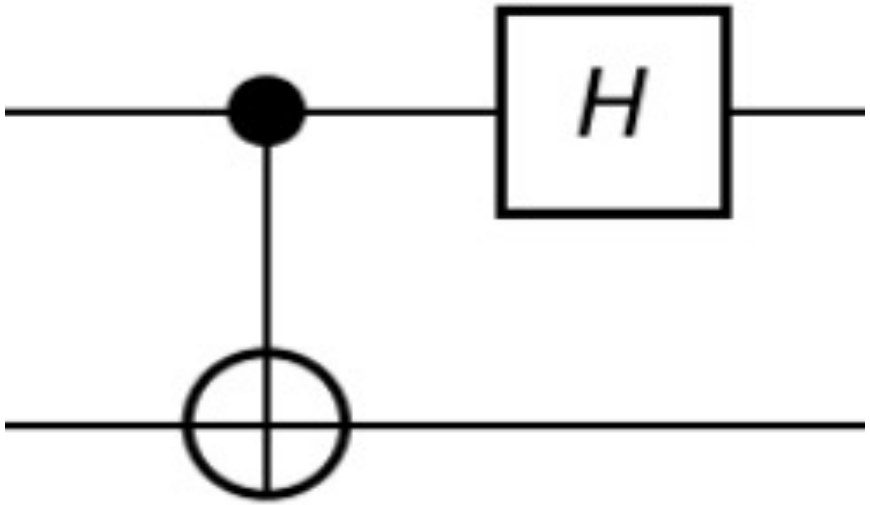
-- Bell State Gate と Bell Measure Gateで
量子テレポーテーション回路を記述する --

Bell State Gateと
Bell Measure Gate

Bell State Gate

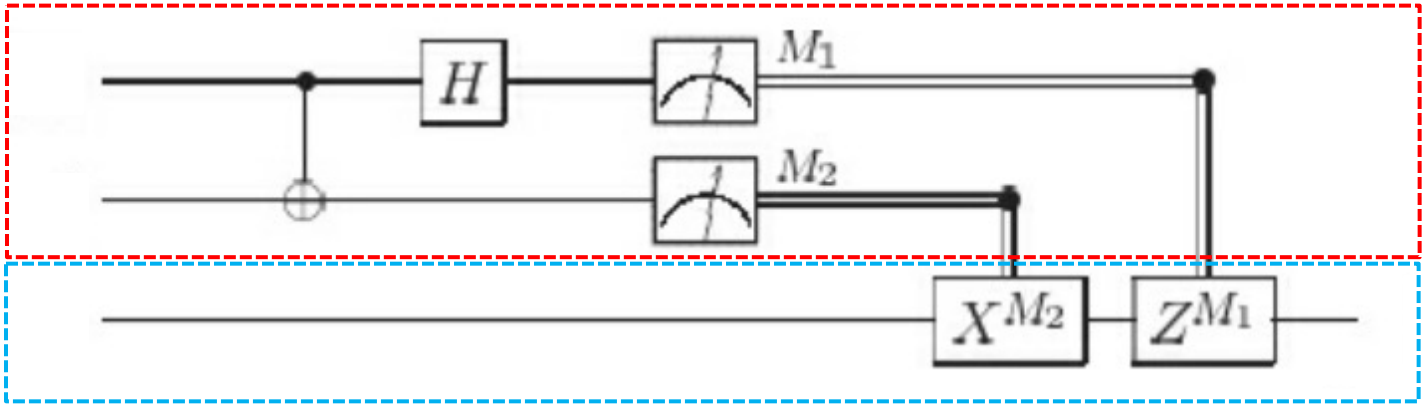


Bell Measure Gate



先に見た量子テレポーテーション回路

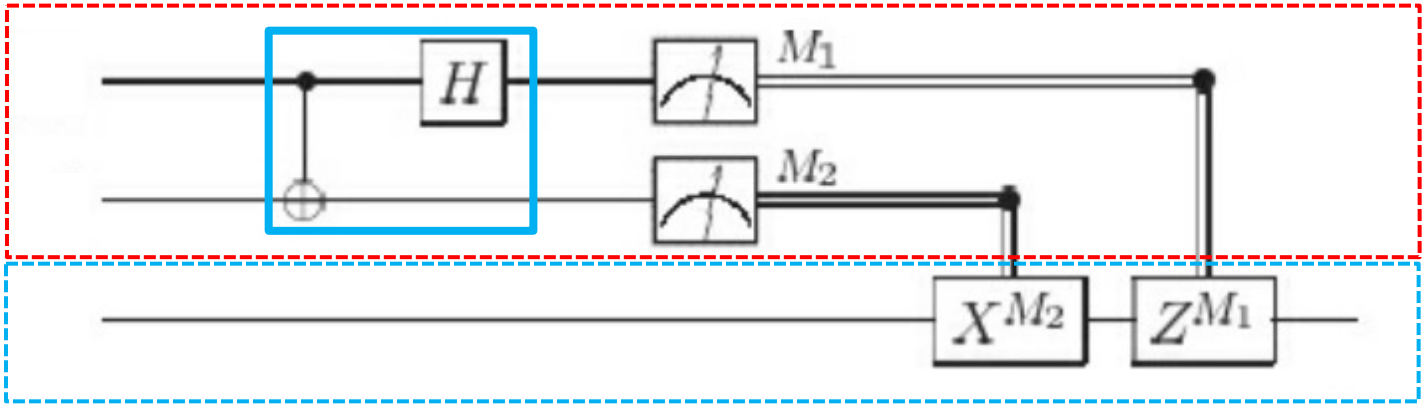
Alice



Bob

この回路には、
Bell Measure Gate が含まれている

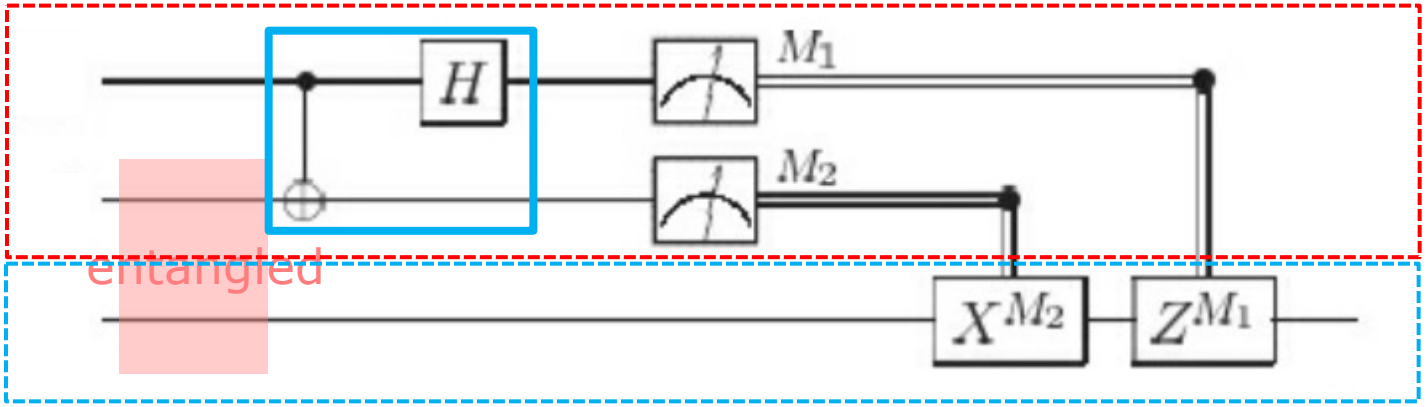
Alice



Bob

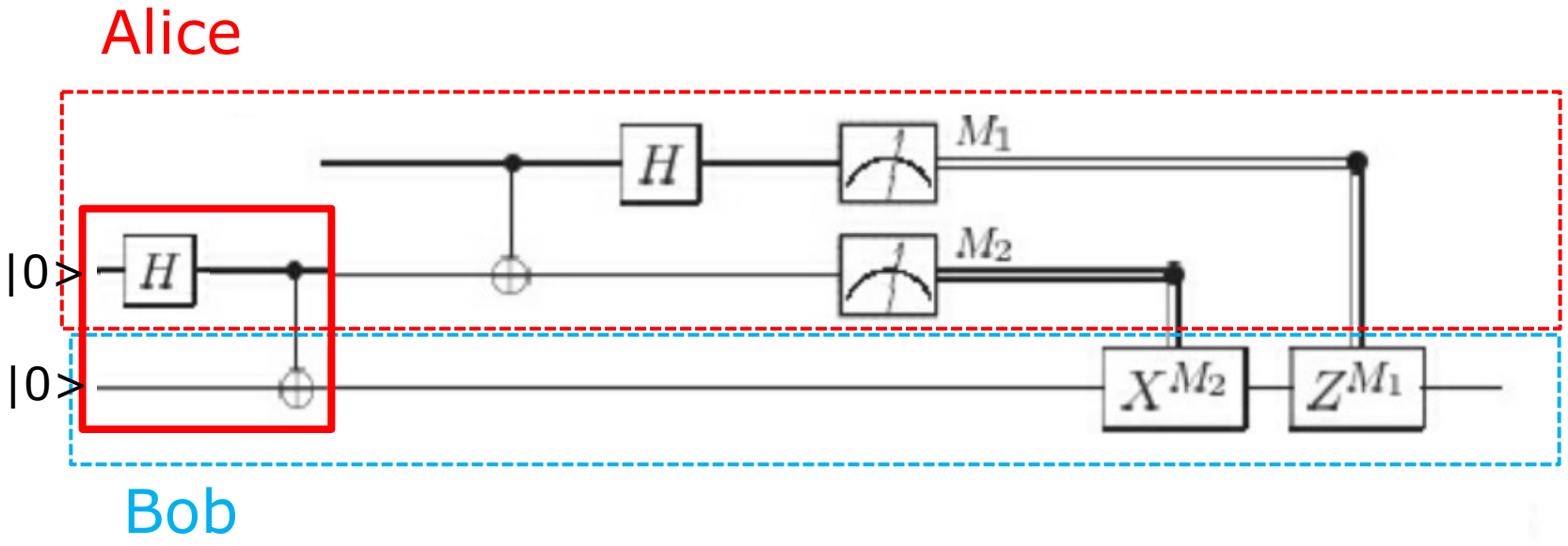
この回路の前提として、
AliceとBobはエンタングルしているという

Alice

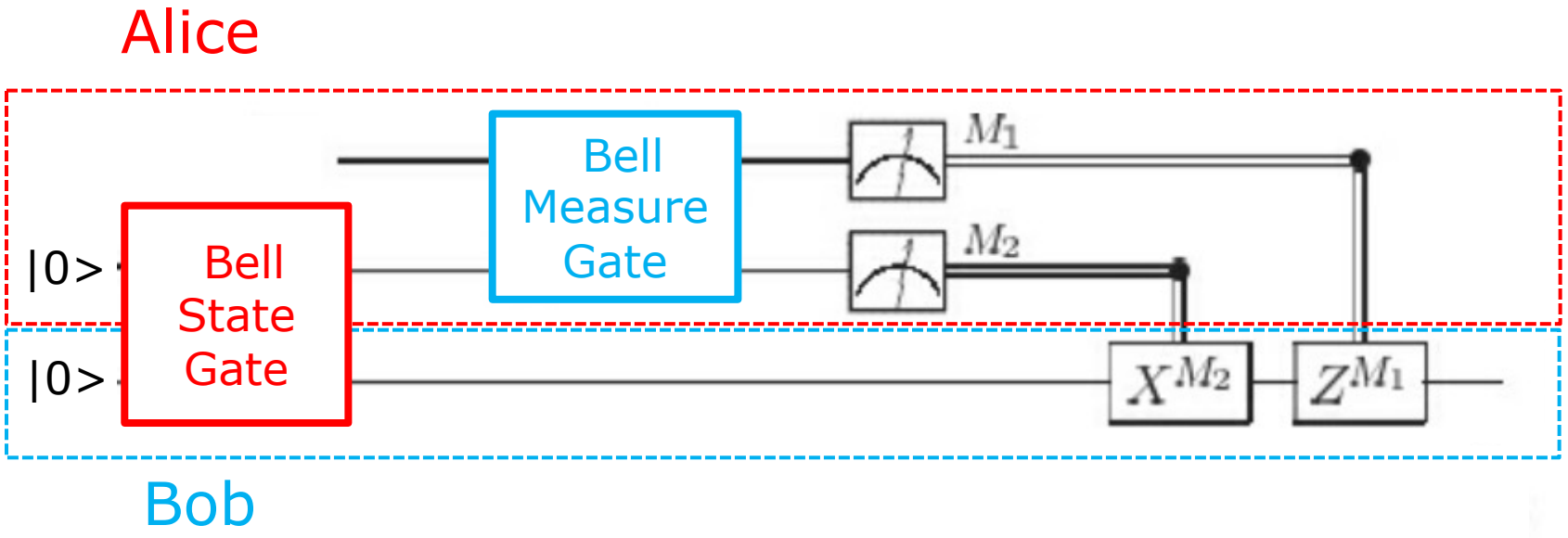


Bob

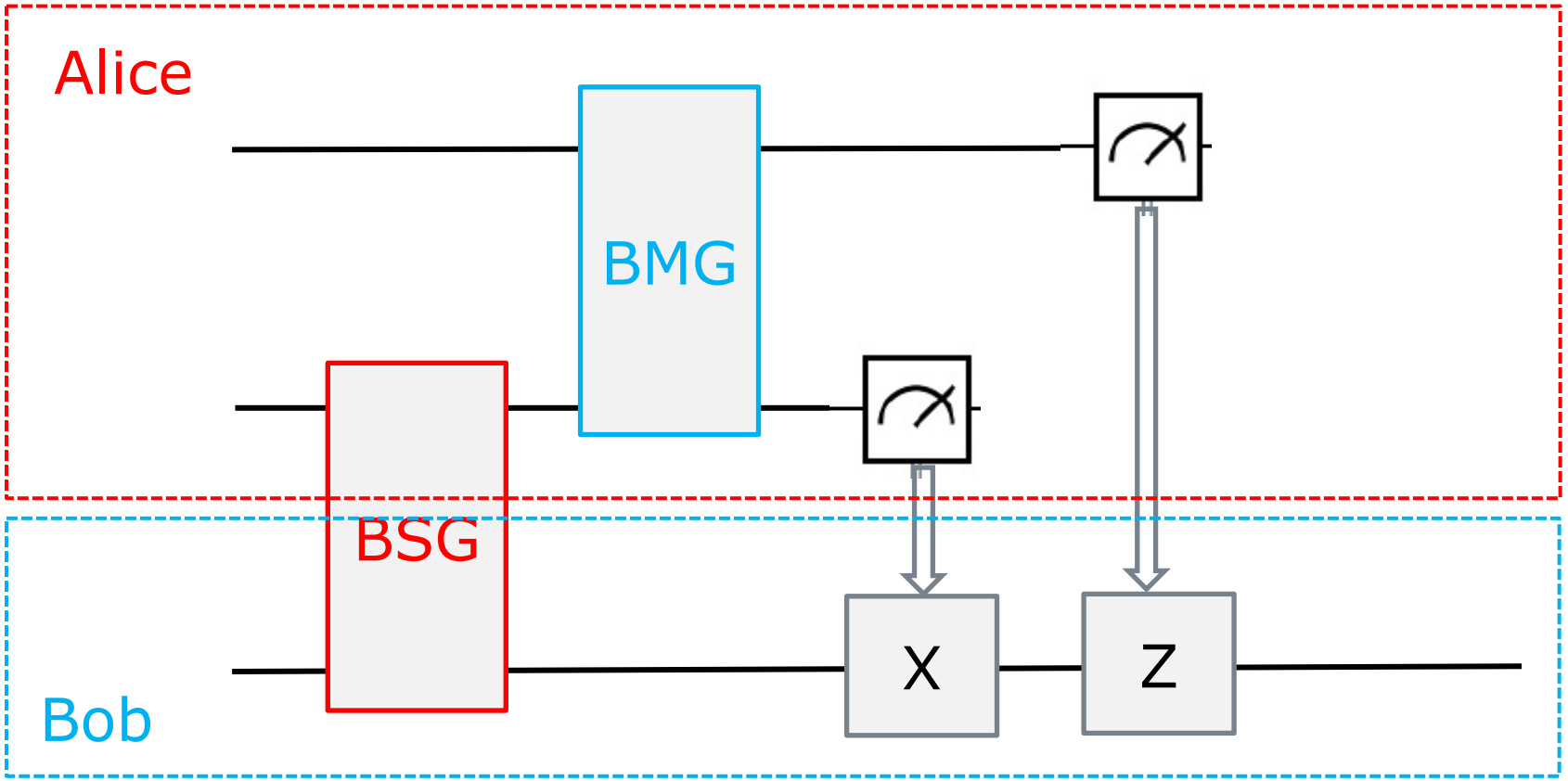
エンタングルメント状態$|\Phi^+>$を生成する回路 Bell State Gate を追加する



Bell Measure GateとBell State Gate をブロックで表わそう



量子テレポーテーション回路



BSG = Bell State Gate
BMG = Bell Measure Gate

Part III

量子通信の技術的基礎

Part III 「量子通信の技術的基礎」の概要

この章では、「量子通信の技術的基礎」として、次の二つの技術をとりあげる。

- Entanglement Swapping
- Time-Bin Encoding

前者(Entanglement Swappingは、Entanglement Pair間の距離を広げ、量子通信のリーチを拡大する基本的な手段である。

後者(Time-Bin Encoding)は、光ファイバー上でのqubitのエンコードの基本的な手段である。

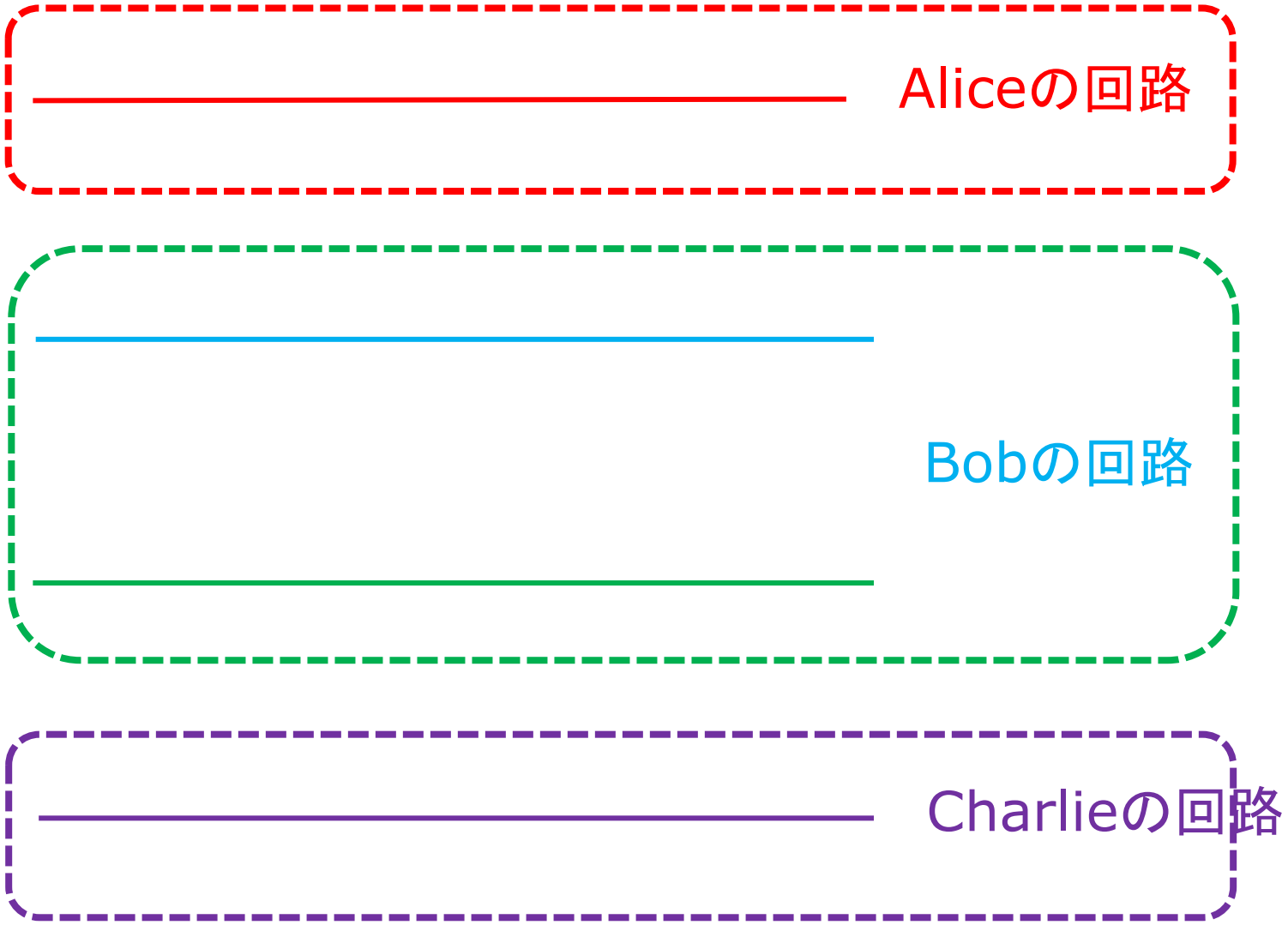
Part III　量子通信の技術的基礎
Agenda

1. Entanglement Swapping
   1. Entanglement Swappingとは何か？
   2. Entanglement Swapping で Entanglementの距離を拡大する
2. Time-Bin Encoding
   1. Mach-Zehnder干渉計
   2. time-bin qubit encoding 回路の形
   3. time-bin encodingの実験

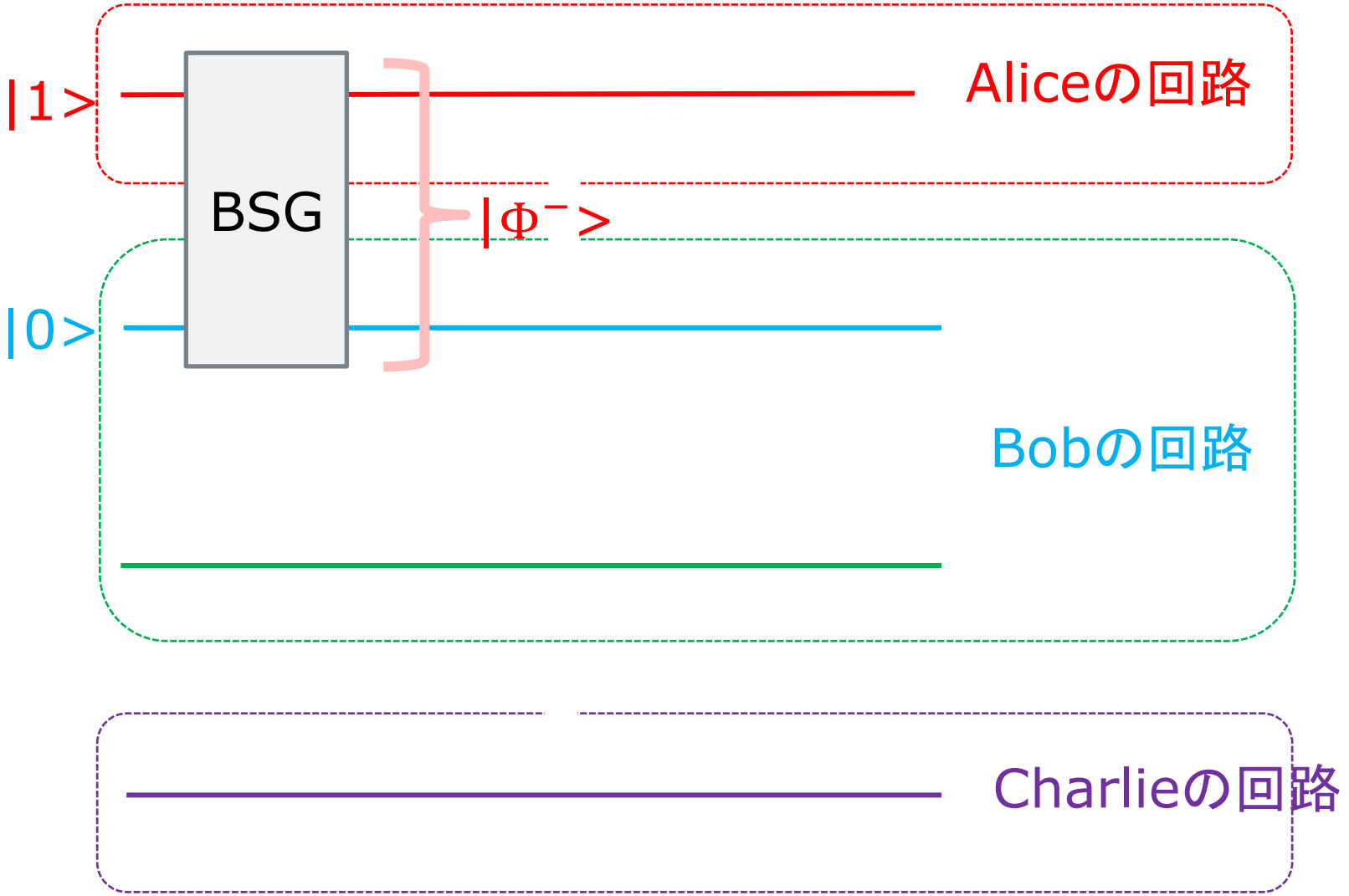

Entanglement Swapping

Entanglement Swappingとは何か？

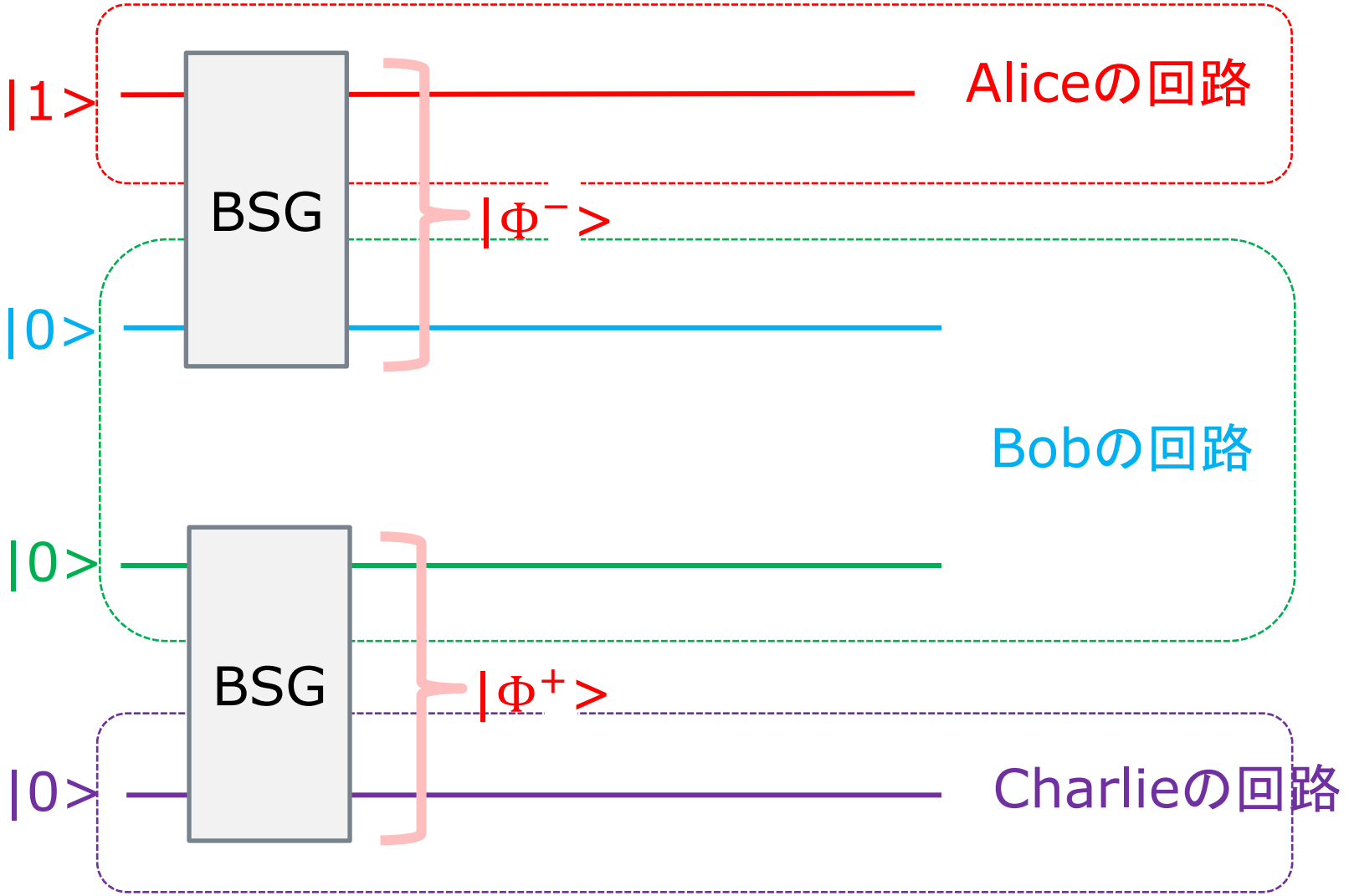
AliceとBobとCharlieが
次のような回路を持っているとしよう



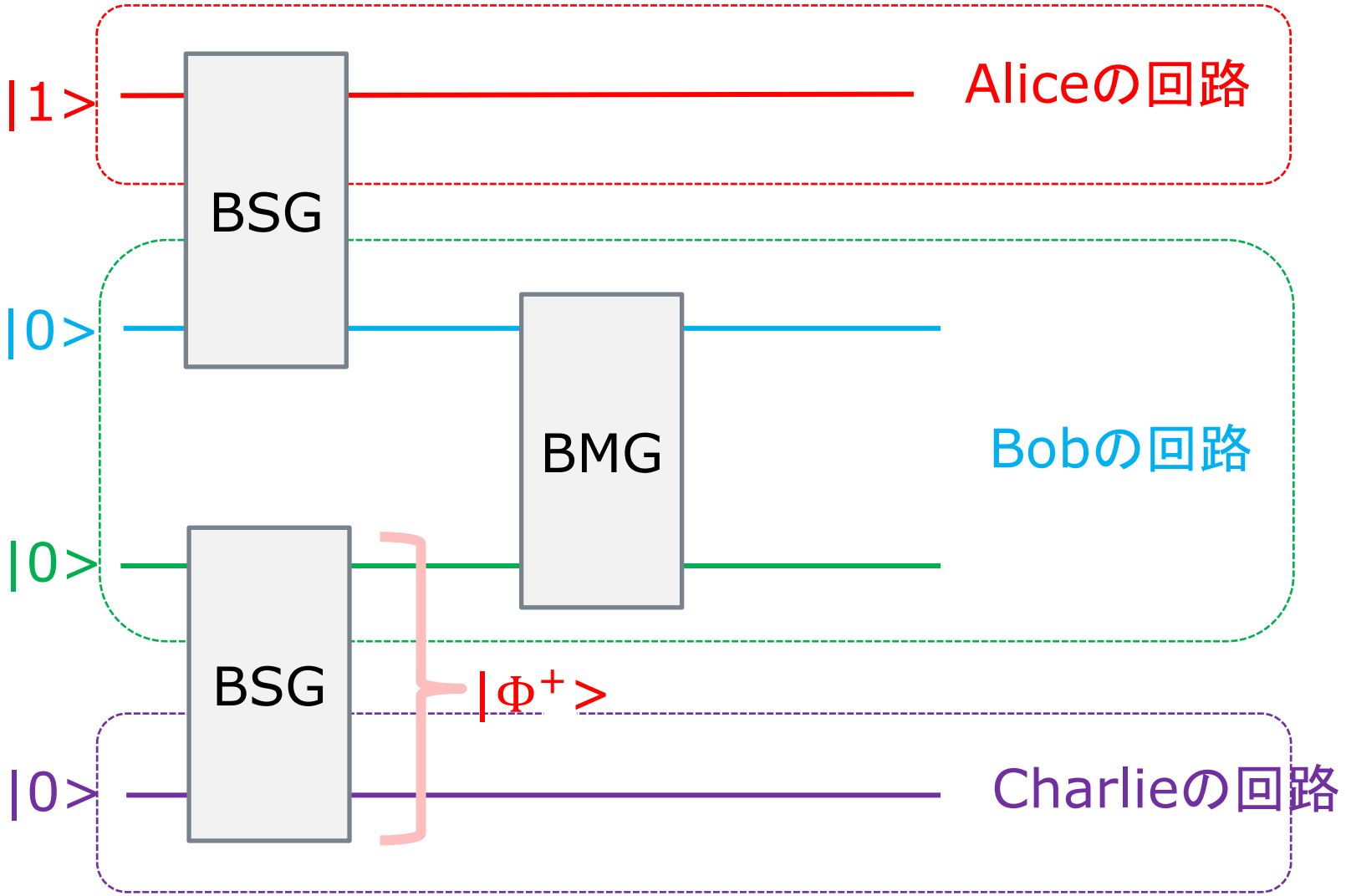
まず、AliceとBobは、Bell State $|\Phi^-\rangle$で、
エンタングルしているとする



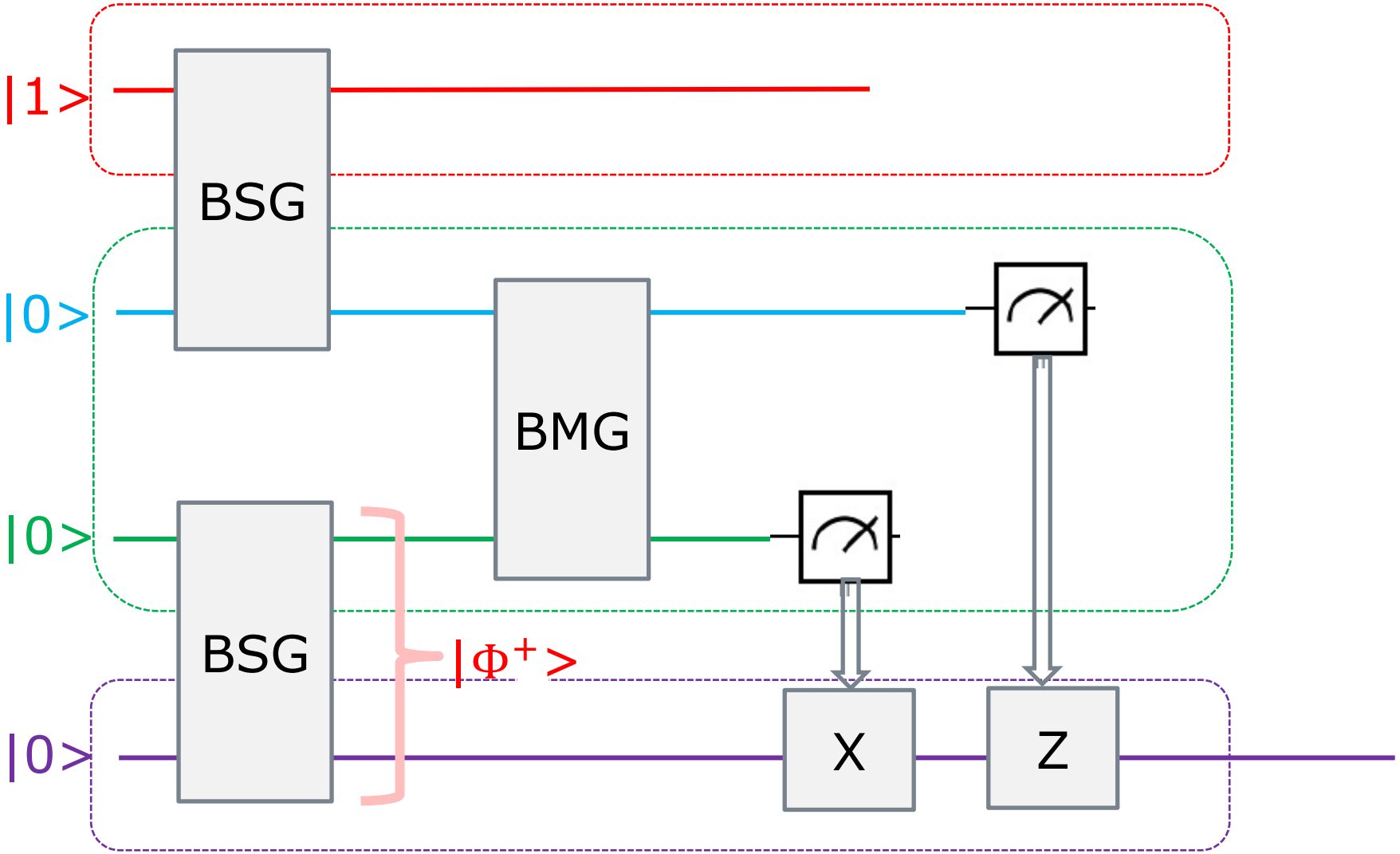
次に、BobとCharlieは、Bell State $|\Phi^+\rangle$ で
エンタングルしているとする



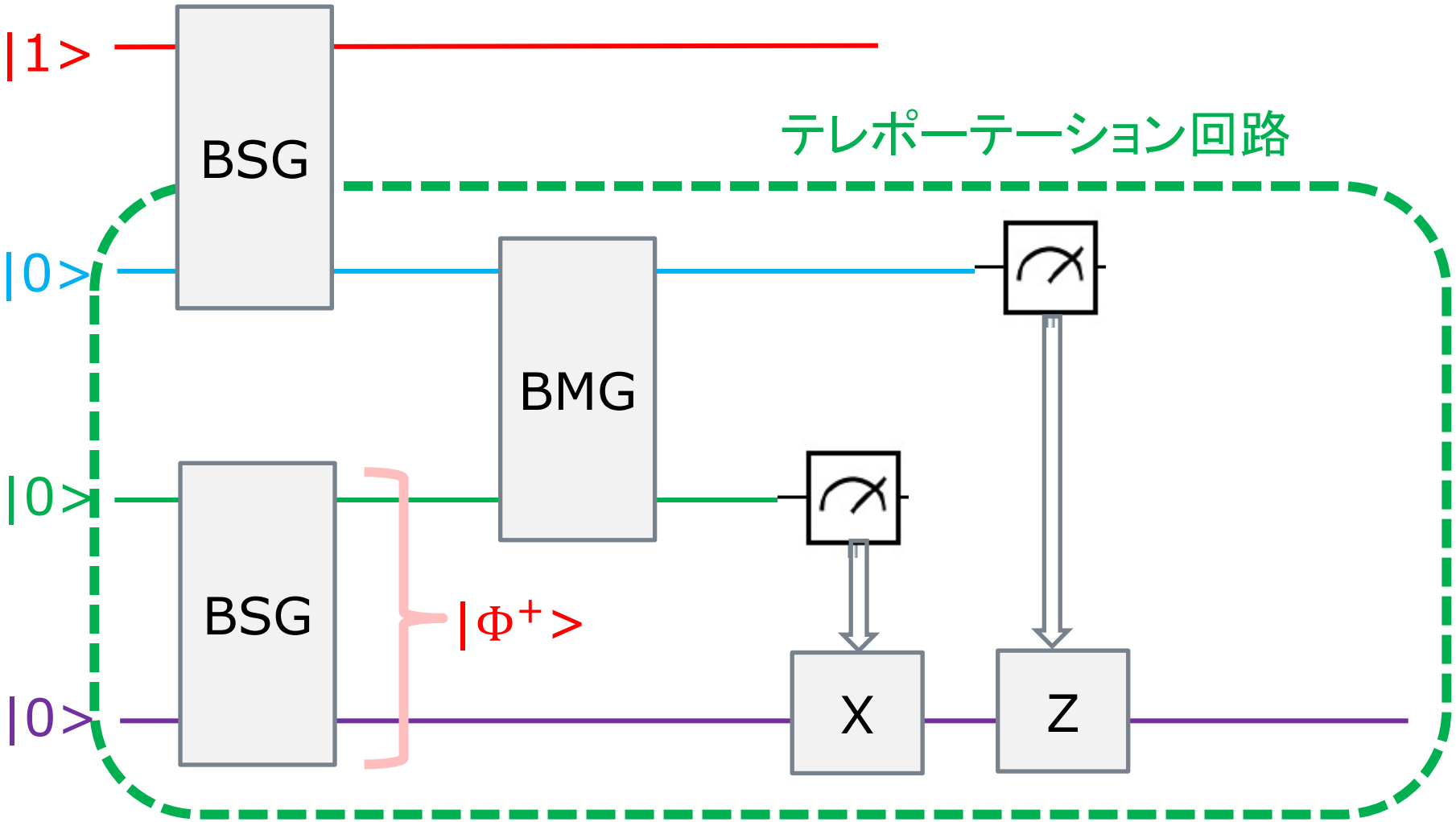
この時、Bobは、$|\Phi^+\rangle$を利用して
テレポーテーション回路を作ることが出来る
前段部



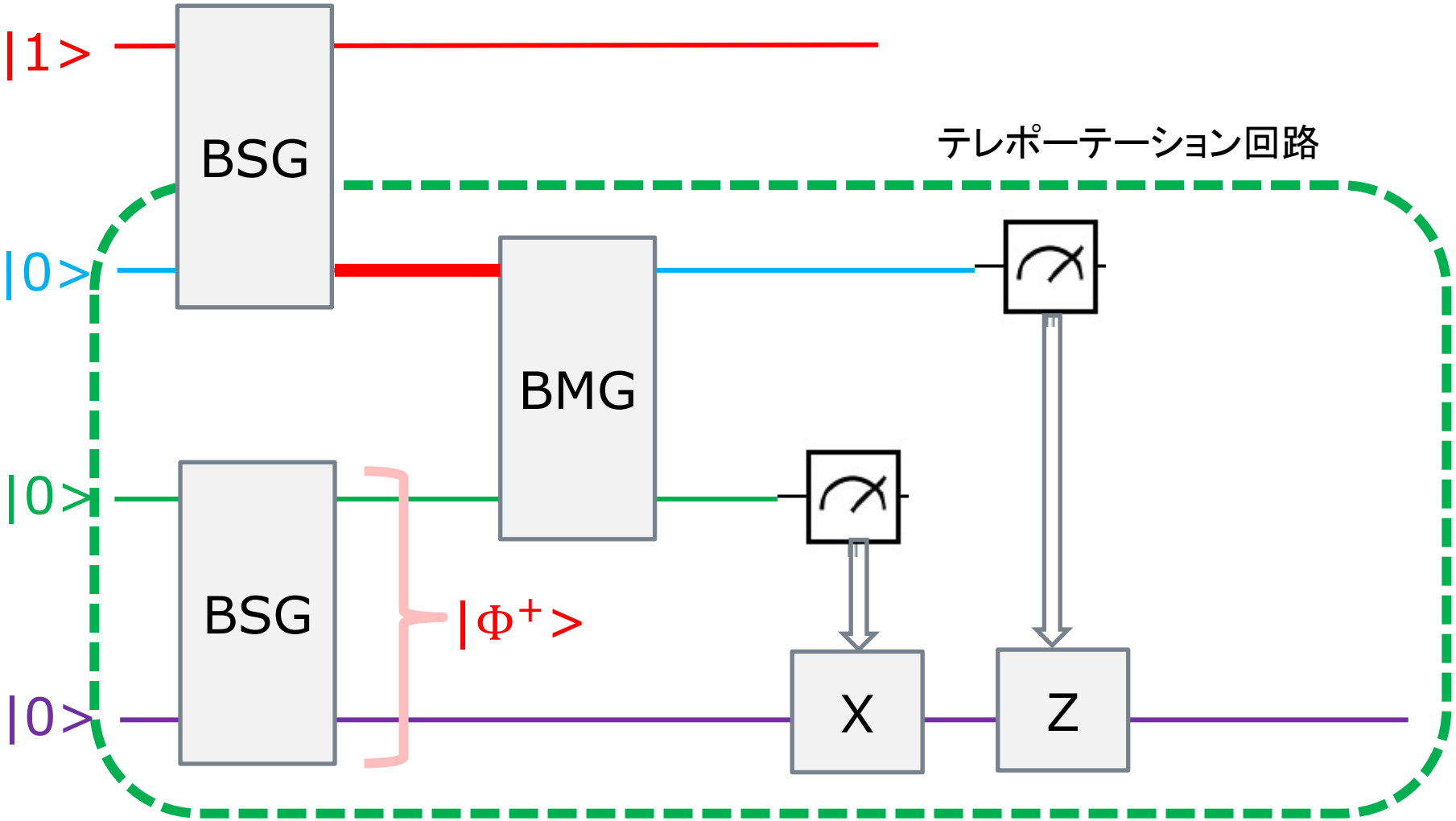
この時、Bobは、$|\Phi^+\rangle$を利用して
テレポーテーション回路を作ることが出来る
後段部



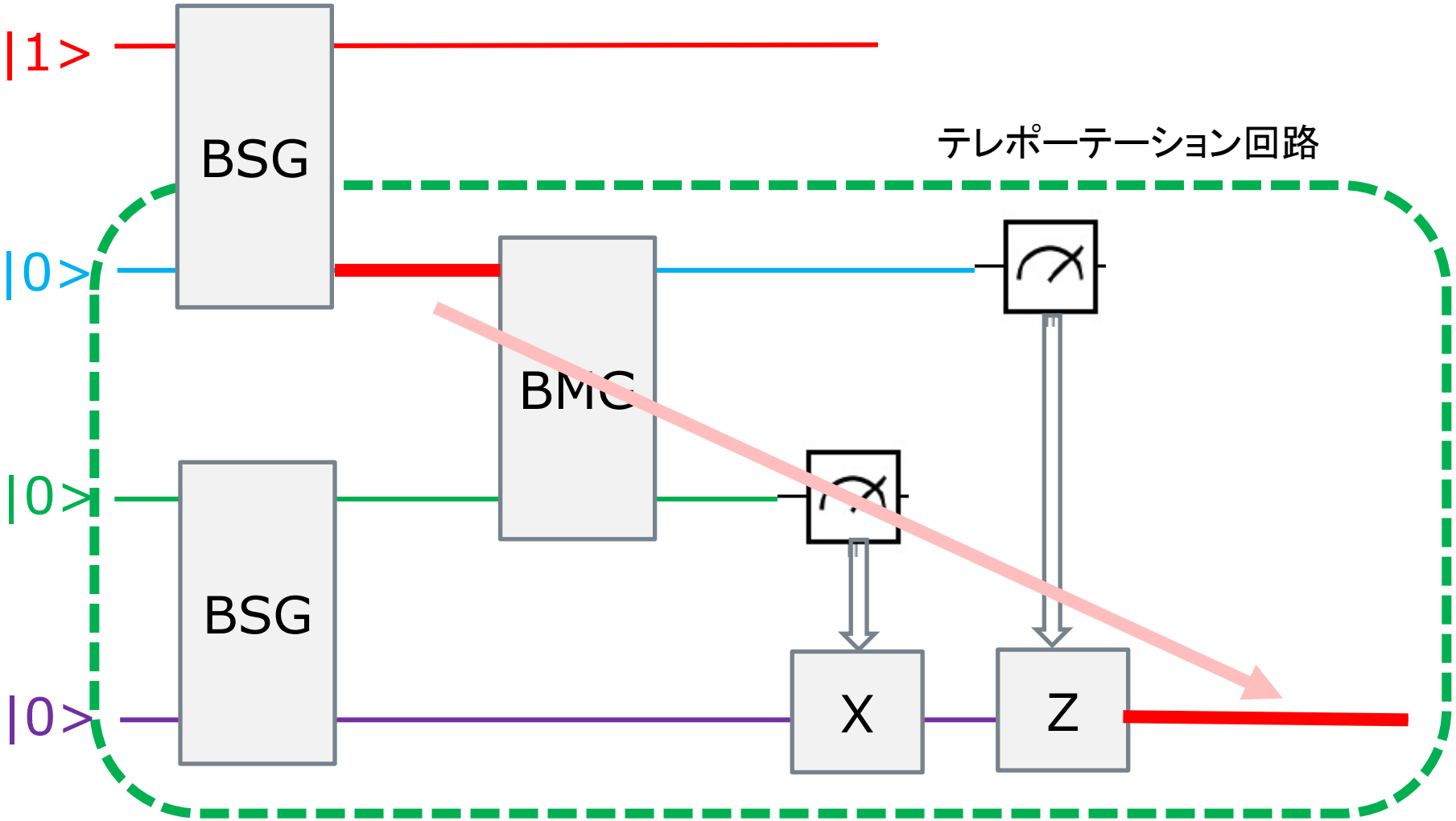
このテレポーテーション回路は、
第二ラインのqubitを第四ラインに送る



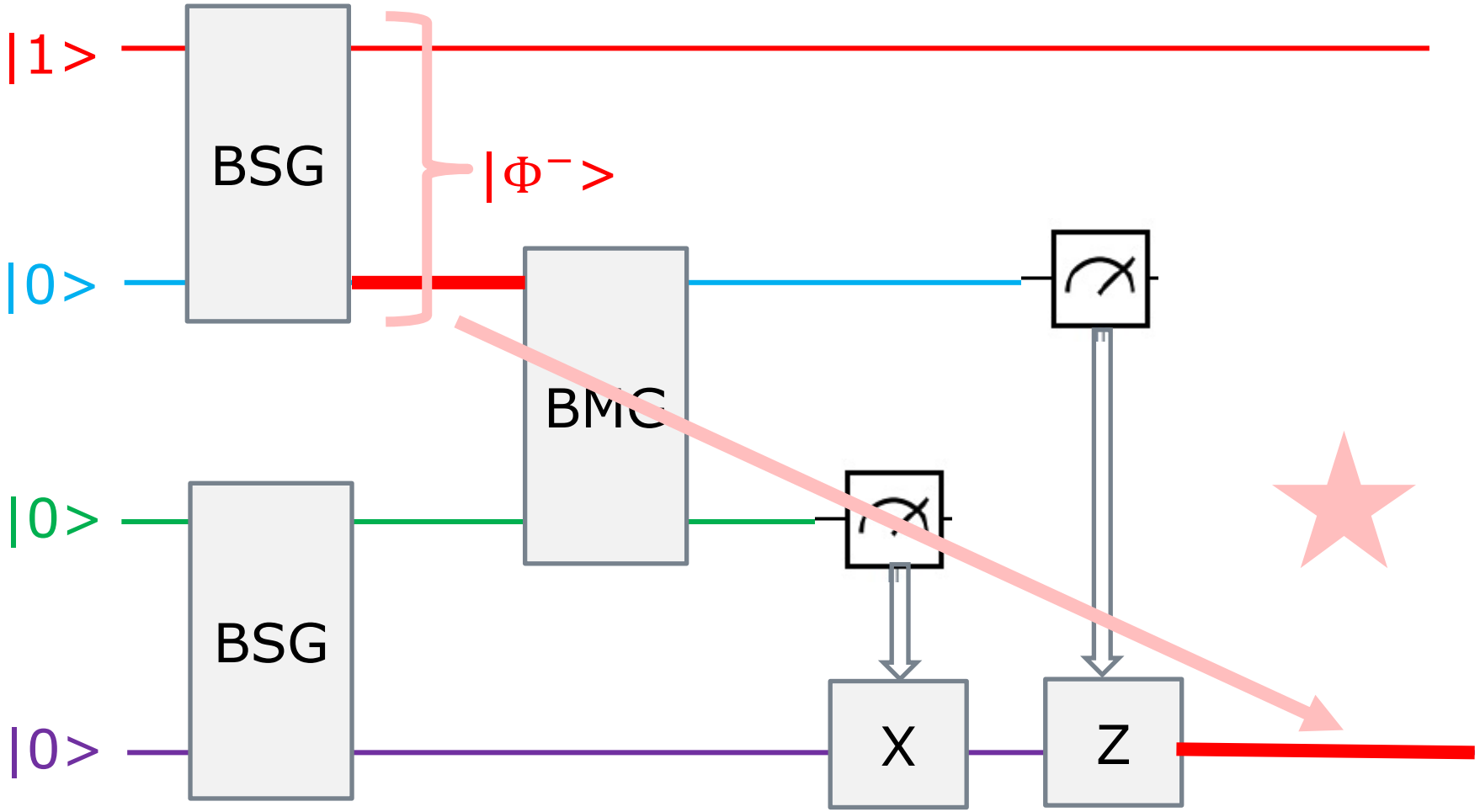
テレポーテーション回路は、
図の赤線部分の状態を転送する



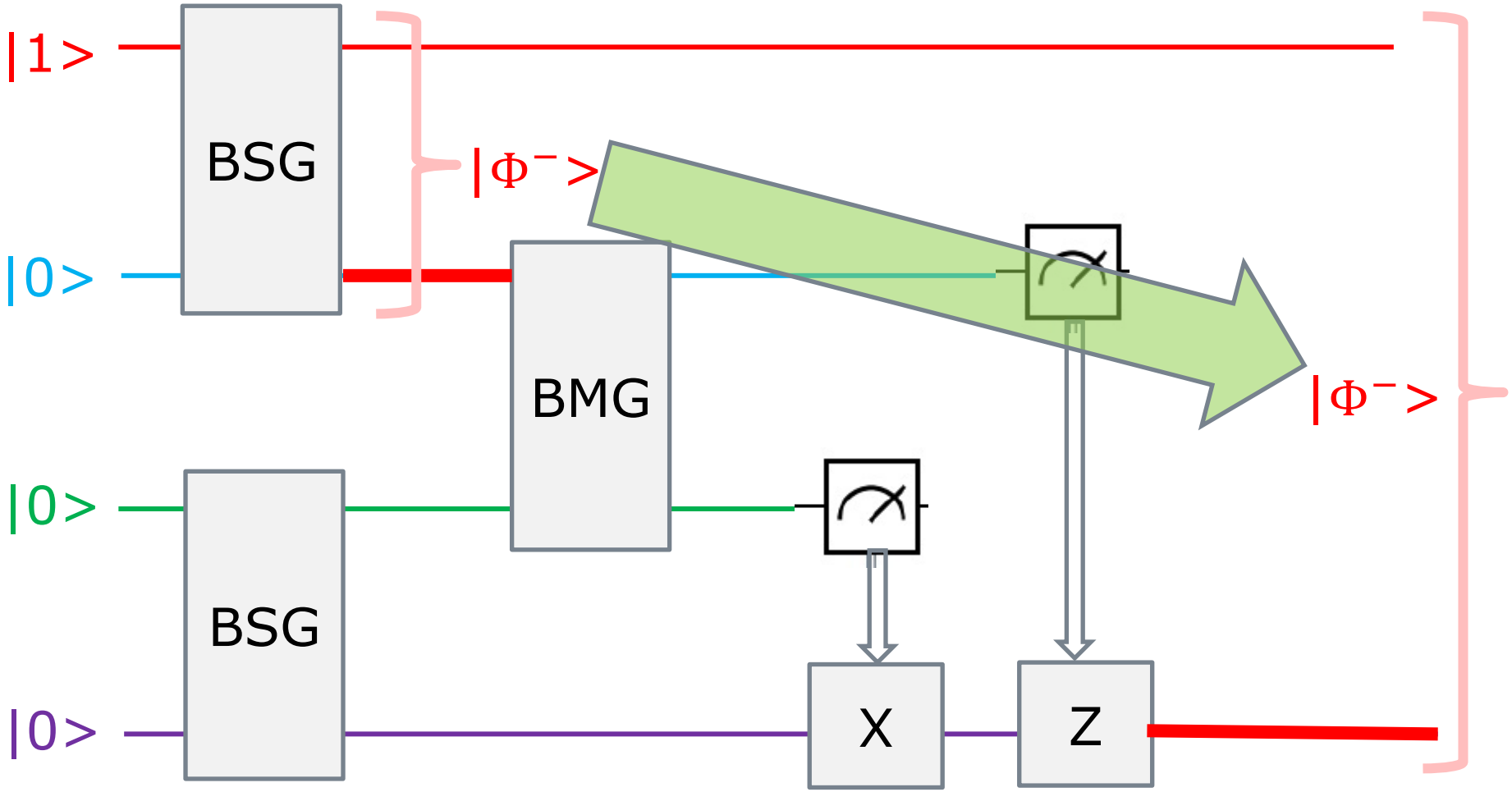
テレポーテーション回路は、
Bobの回路からCharlieの回路に
図の赤線部分の状態を転送する



Aliceと図の赤線部分の関係は、
$|\Phi^-\rangle$ のエンタングルメント状態である



その状態は、Charlieに移った。
AliceとCharlieは、エンタングルメント状態になる。



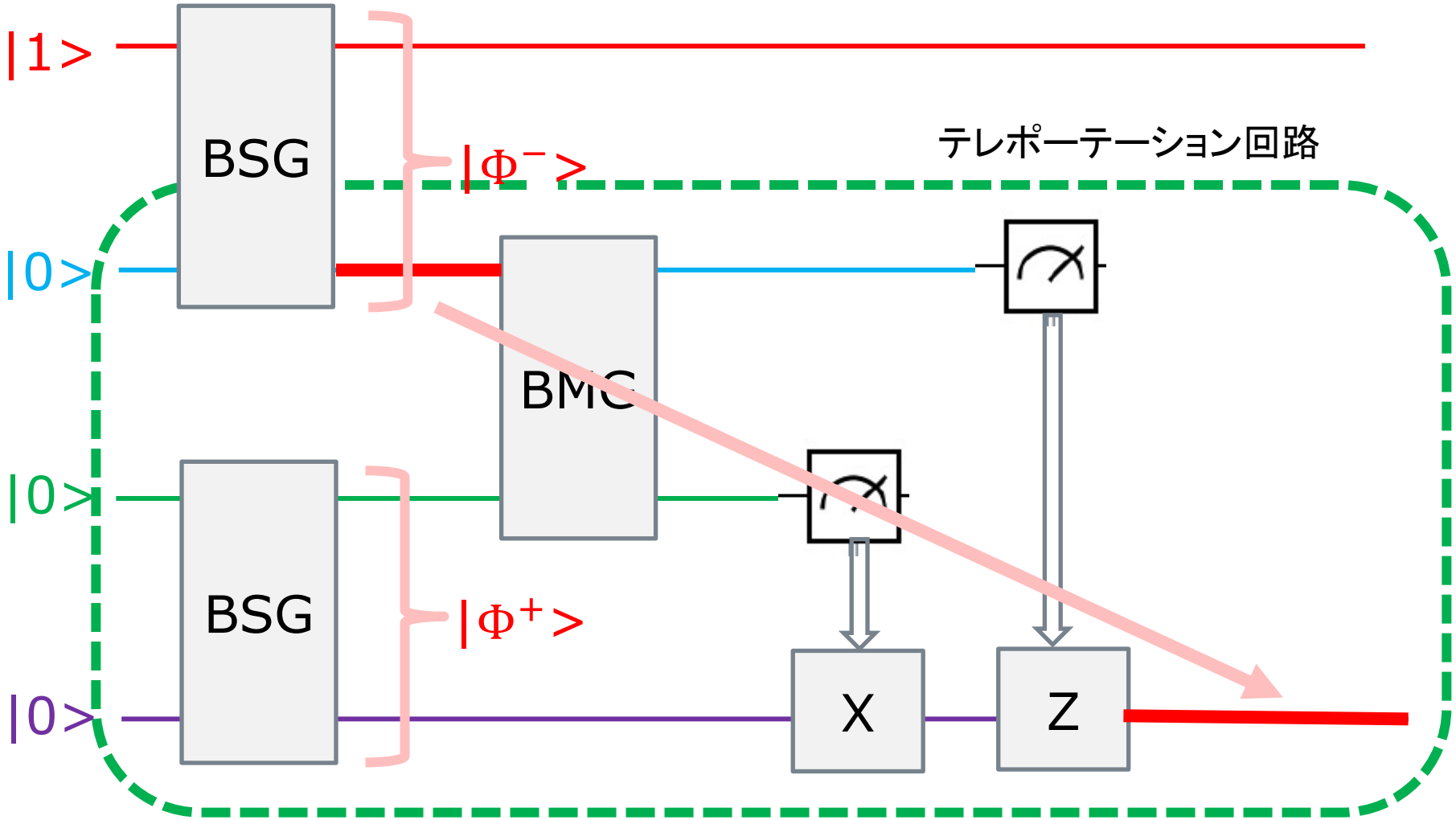
Entanglement Swappingの奇妙さ

- 最初は、エンタングルメント状態にあったのは、AliceとBobの間と、BobとCharlieの間である。AliceとCharlieはエンタングルメント状態にはない。
- Bobは自分の回路上で、第二ラインと第三ライン上で、観測を行って、その結果をCharlieに送る。Charlieは、その情報で、第四ラインのqubitを操作する。これは、BobとCharlieとの間の量子テレポーテーションである。
- ところが、これらの観測・通信・ゲート操作とは関係のなかった、Aliceが、Charlieとエンタングルメント状態に入る。
- 観測・qubit操作によって、もとの Alice-Bob, Bob-Charlie のエンタングルメント状態は、なくなってしまう。

Entanglement Swappingで Entanglementの距離を拡大する

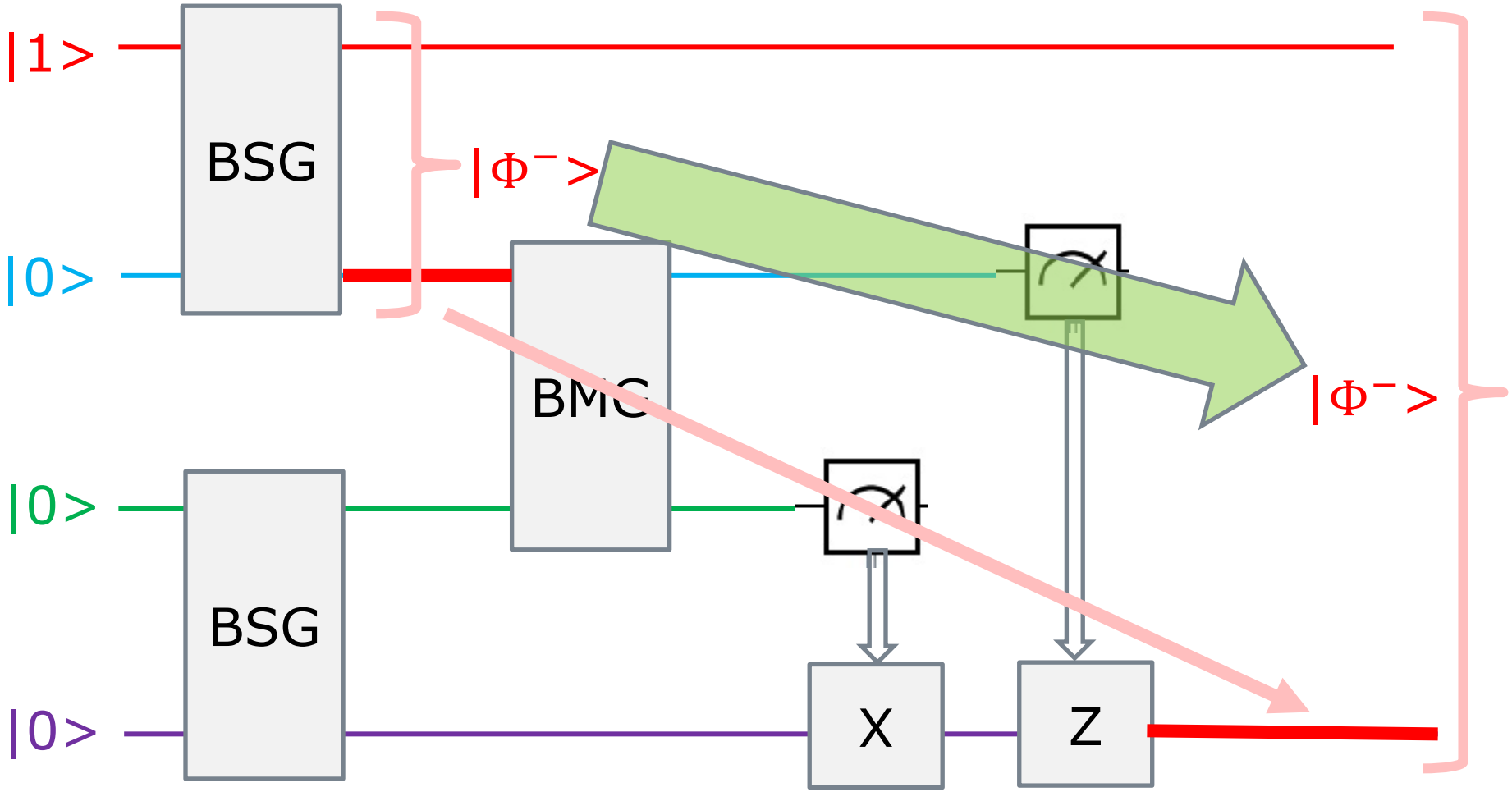
Entanglement Swapping回路

量子テレポーテーションを行うと

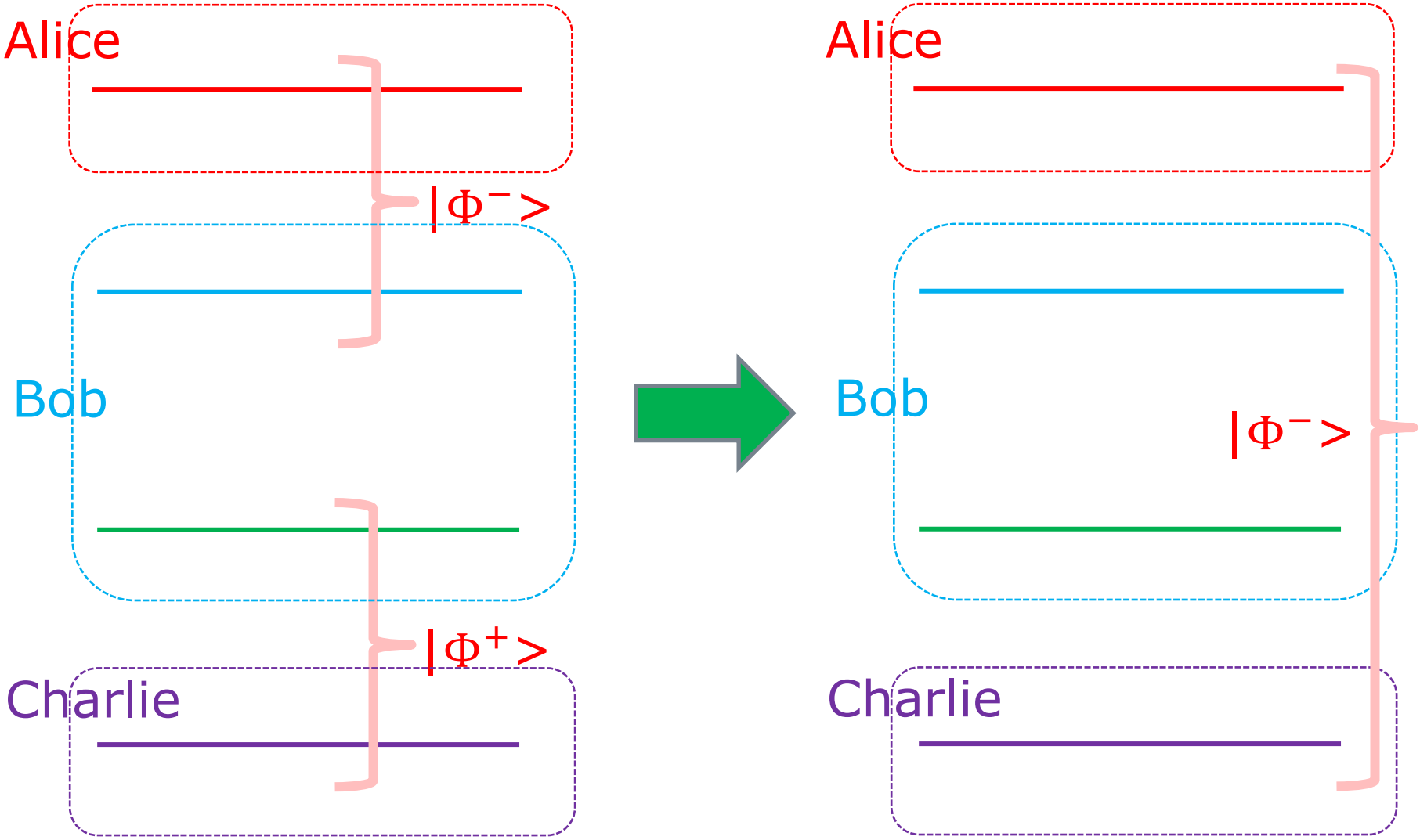


Entanglement Swapping回路

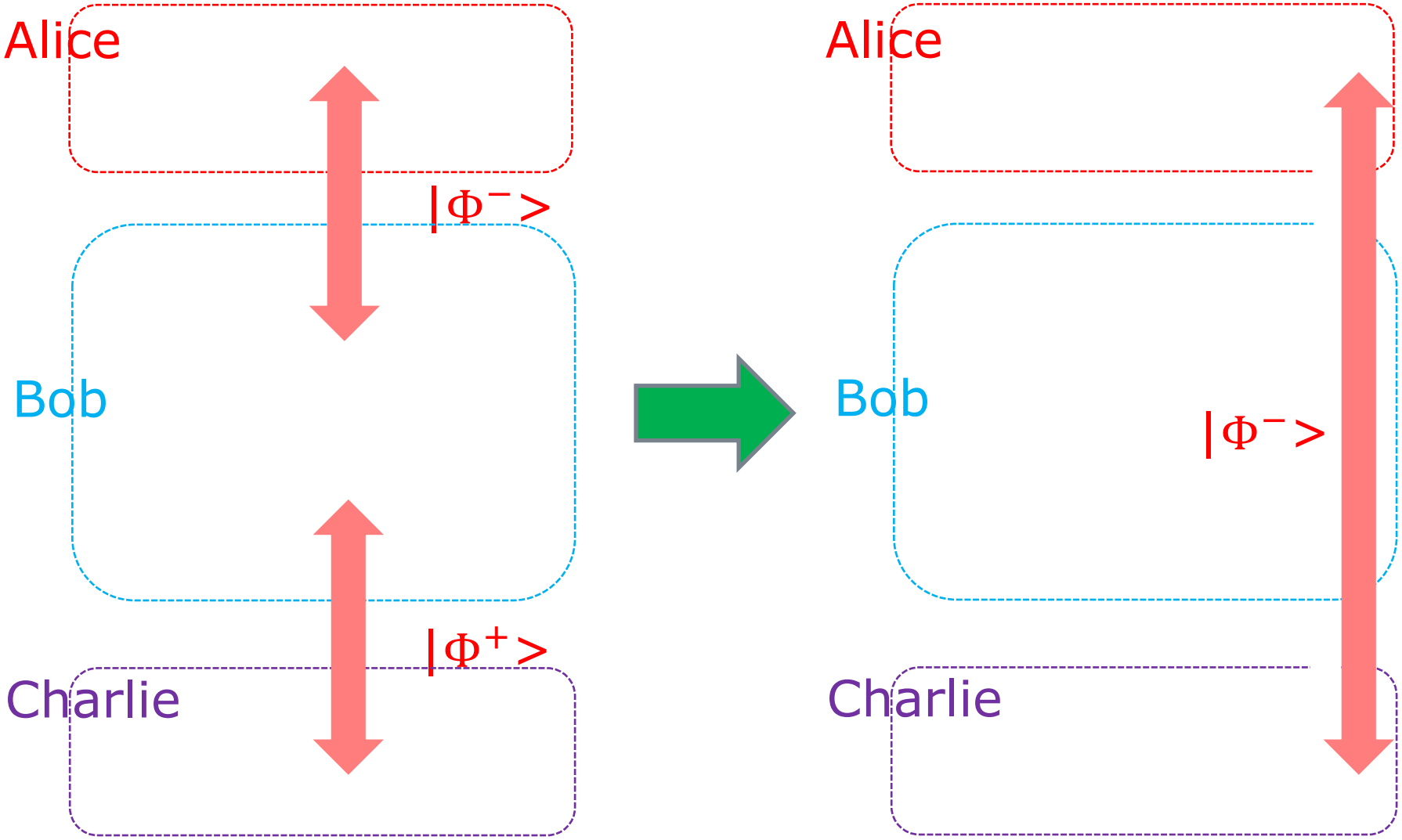
エンタングルメントが移動する



Entanglement Swapping

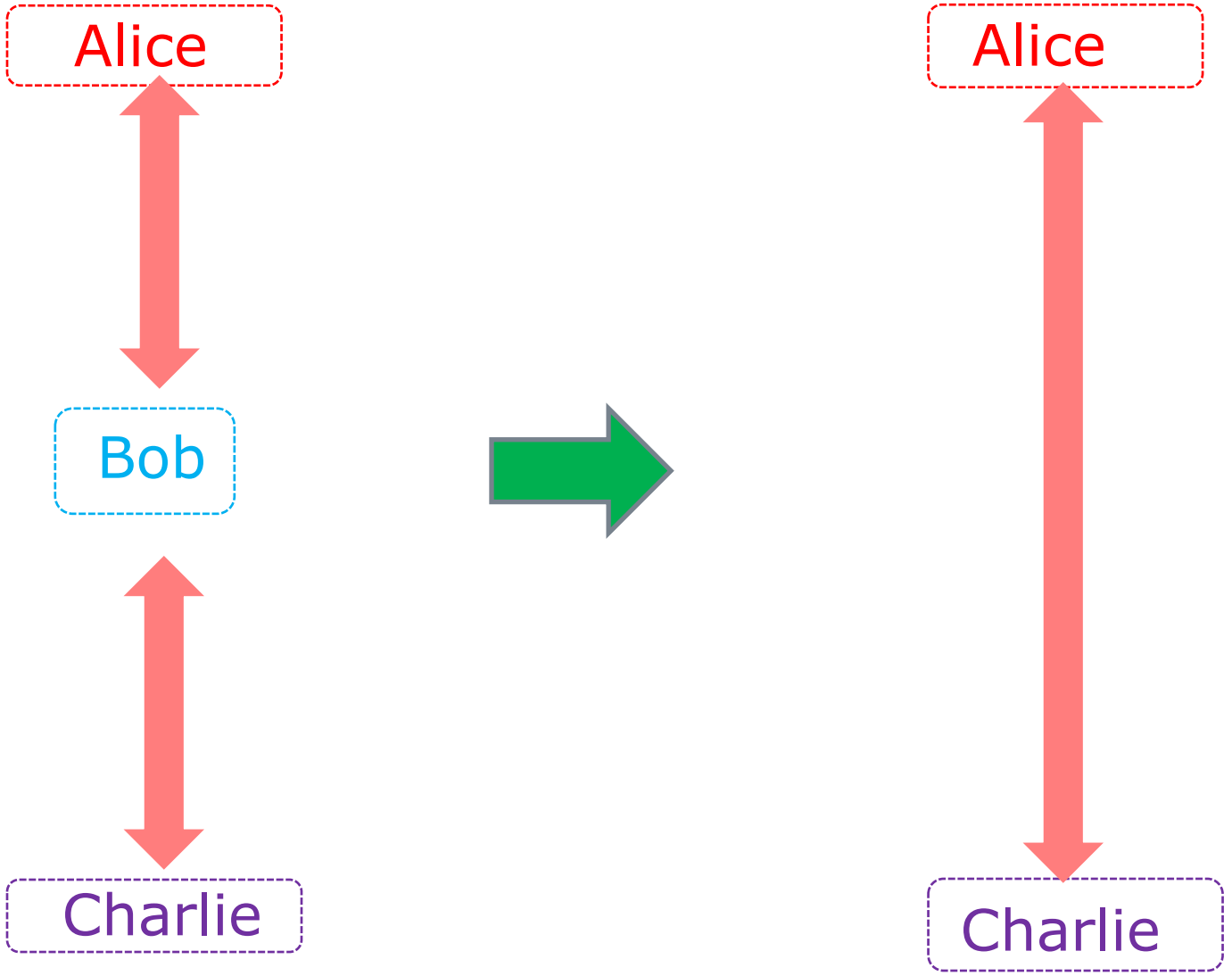


Entanglement Swapping

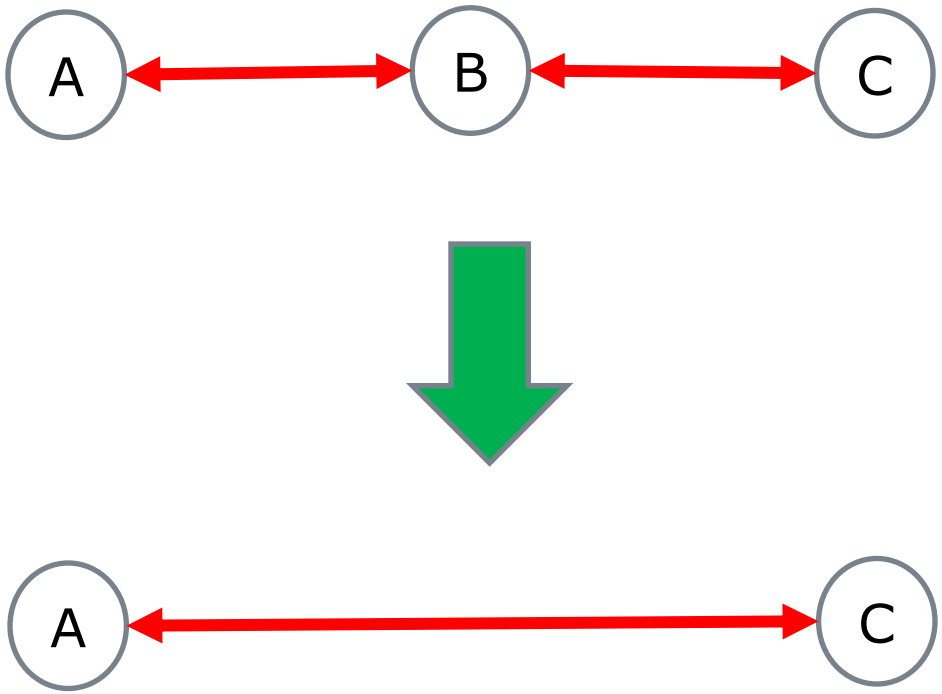


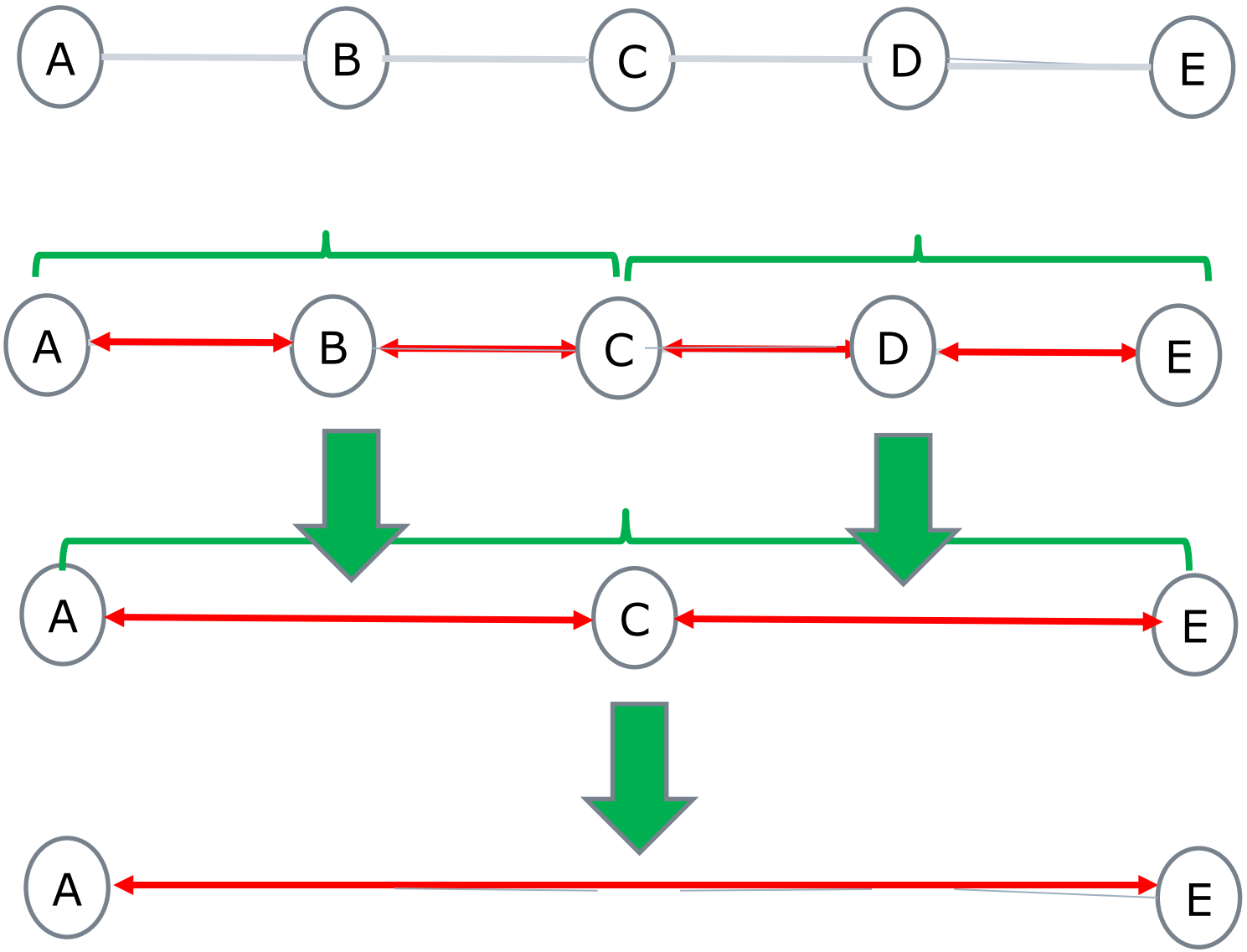
Entanglement Swappingで Entanglementの距離を拡大する

Entanglement Swappingで Entanglementの距離を拡大する



Entanglement Swappingで Entanglementの距離を拡大する




A
B
C
D
E
A
B
C
D
E
A
C
E
A
E


Time-Bin Encoding

qubitの情報を光ファイバーにのせるMach-Zehnder干渉計

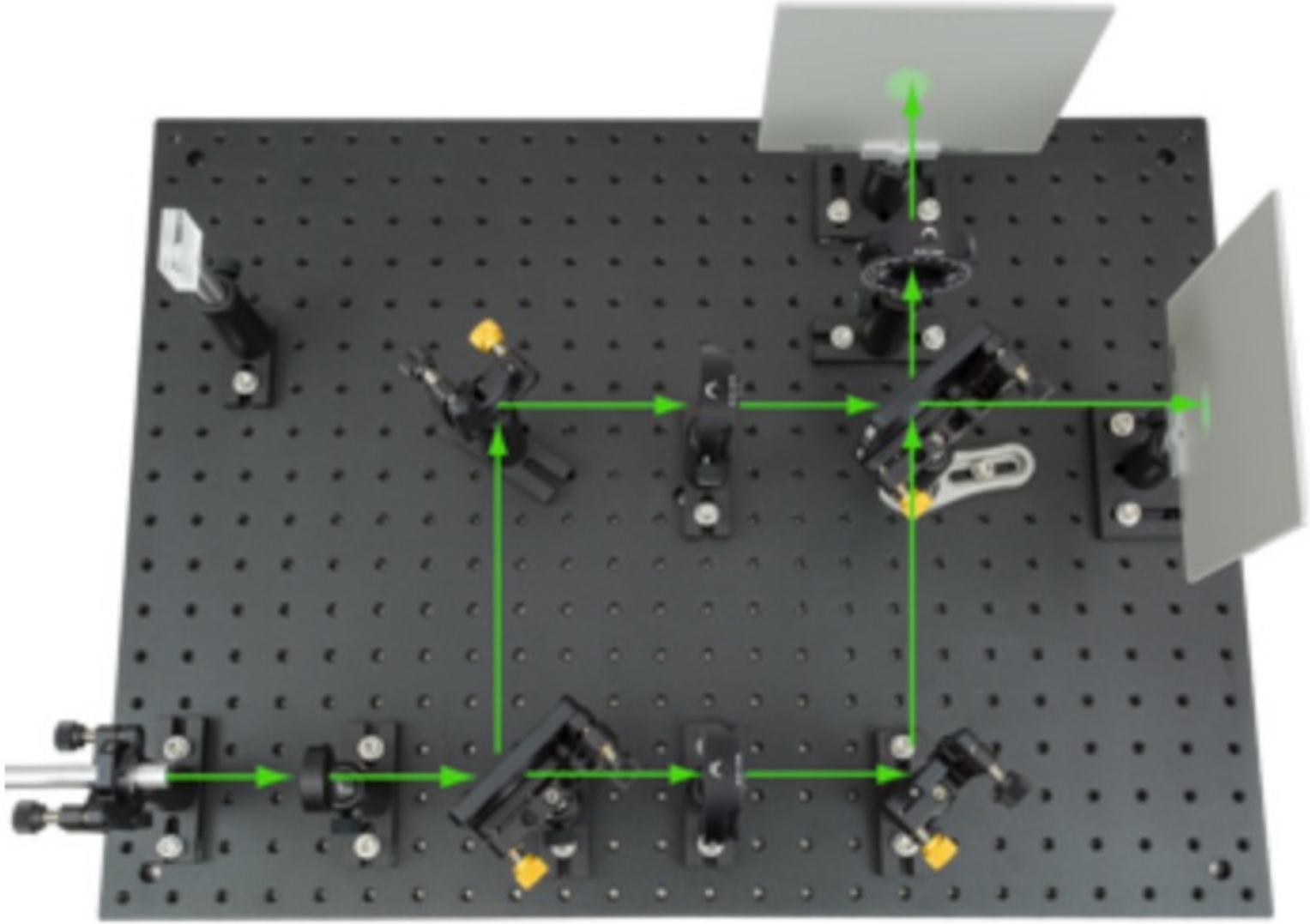
time-bin qubit encoding と Mach-Zehnder 干渉計

この節では、光ファイバーにqubitの情報をのせる手段としての time-bin qubit encoding を紹介する。

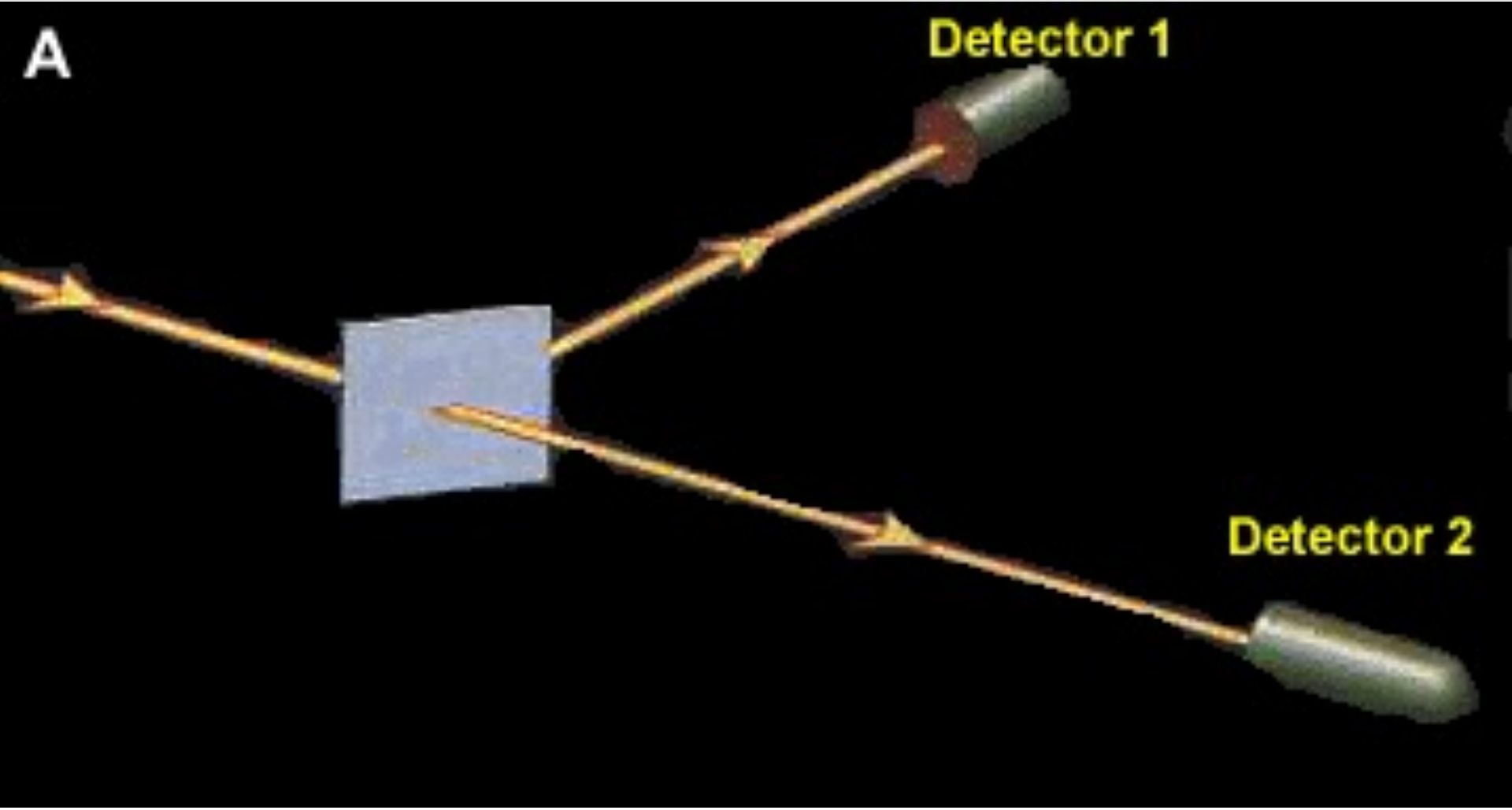
ここでは、time-bin qubit encoding の基礎になっている Mach-Zehnder 干渉計の働きを学ぶ。

Mach Zehnder 干渉計の実験

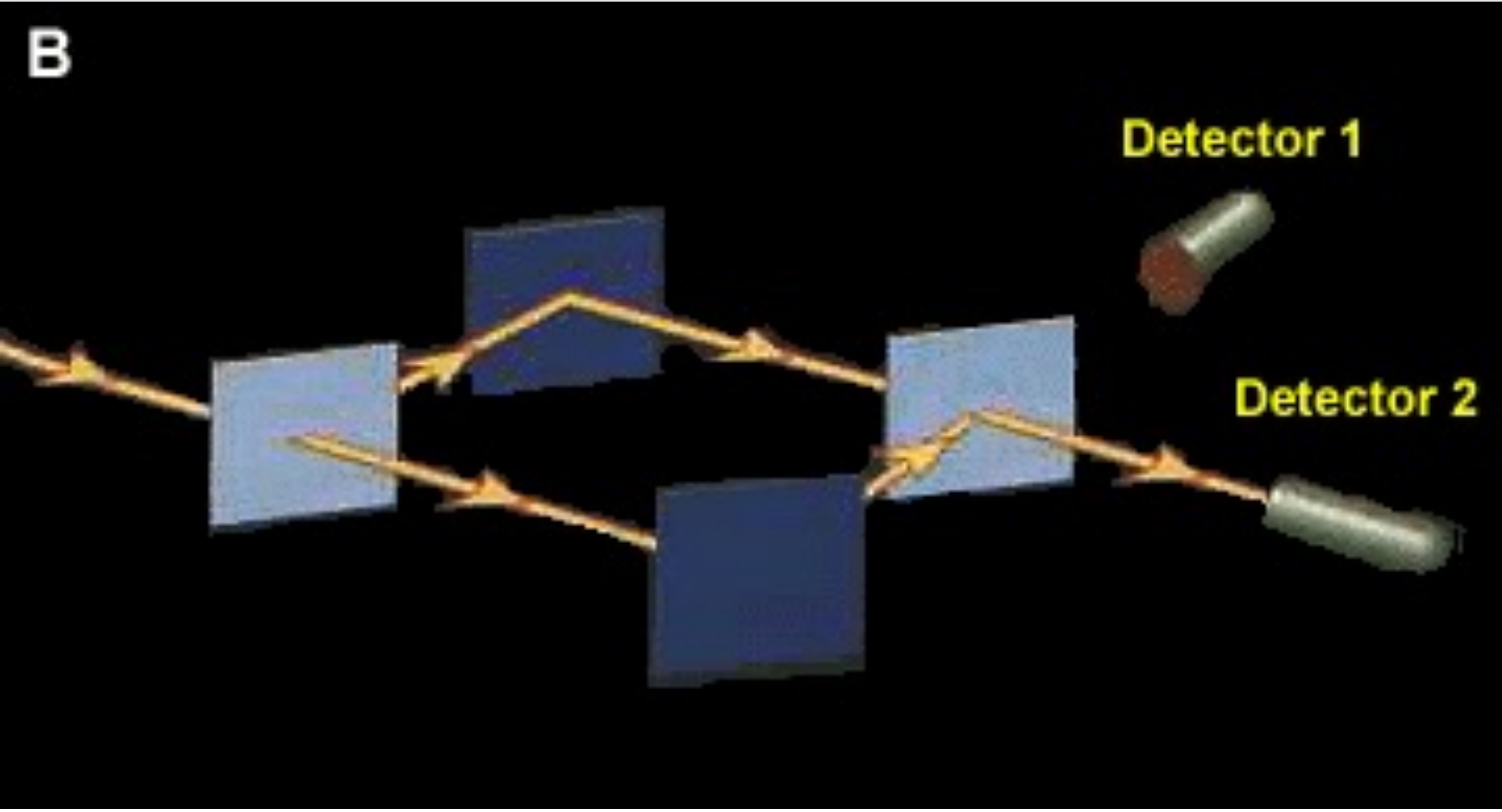
Mach Zehnder 干渉計



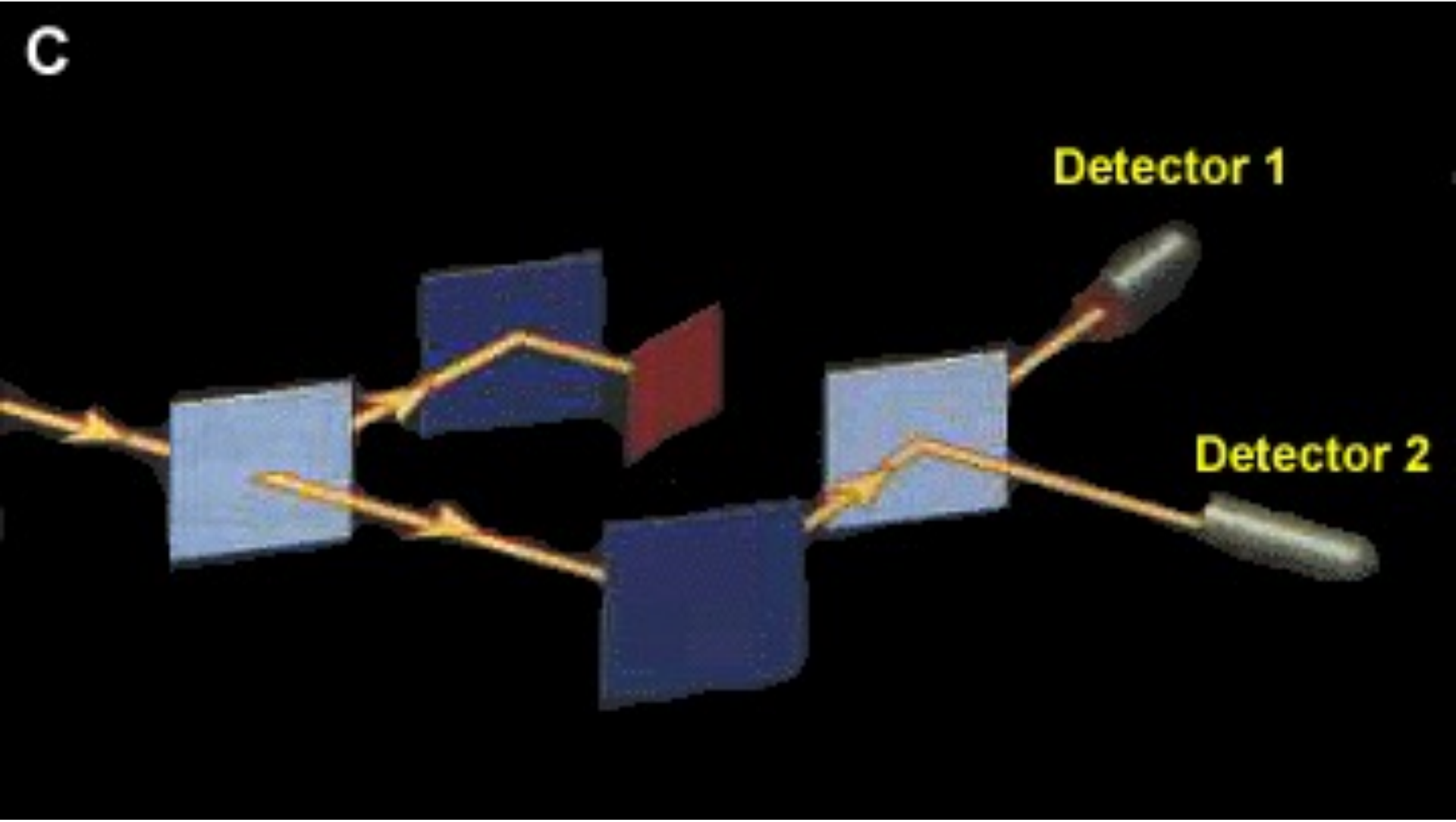
量子消しゴム(Quantum Eraser)実験キット
https://goo.gl/BB4F5D



光を半分は通し半分は反射する、ハーフミラーを45度の角度で光の進路に置く。光は、二つの検出器に届く。光子一個で実験を繰り返すと、ある光子は検出器1に、ある光子は検出器2に届く。その確率は等しい。ここに不思議なことはない。

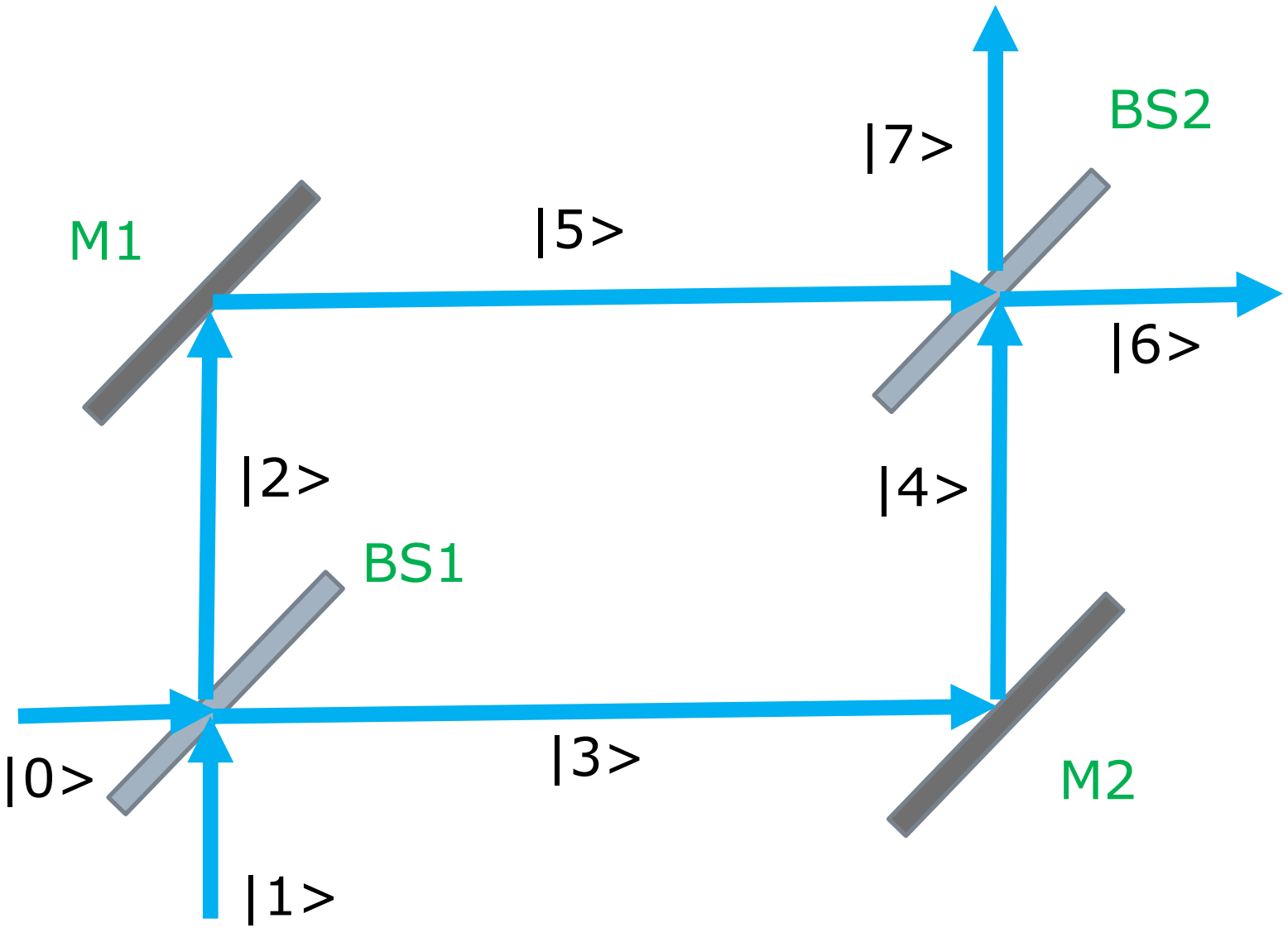


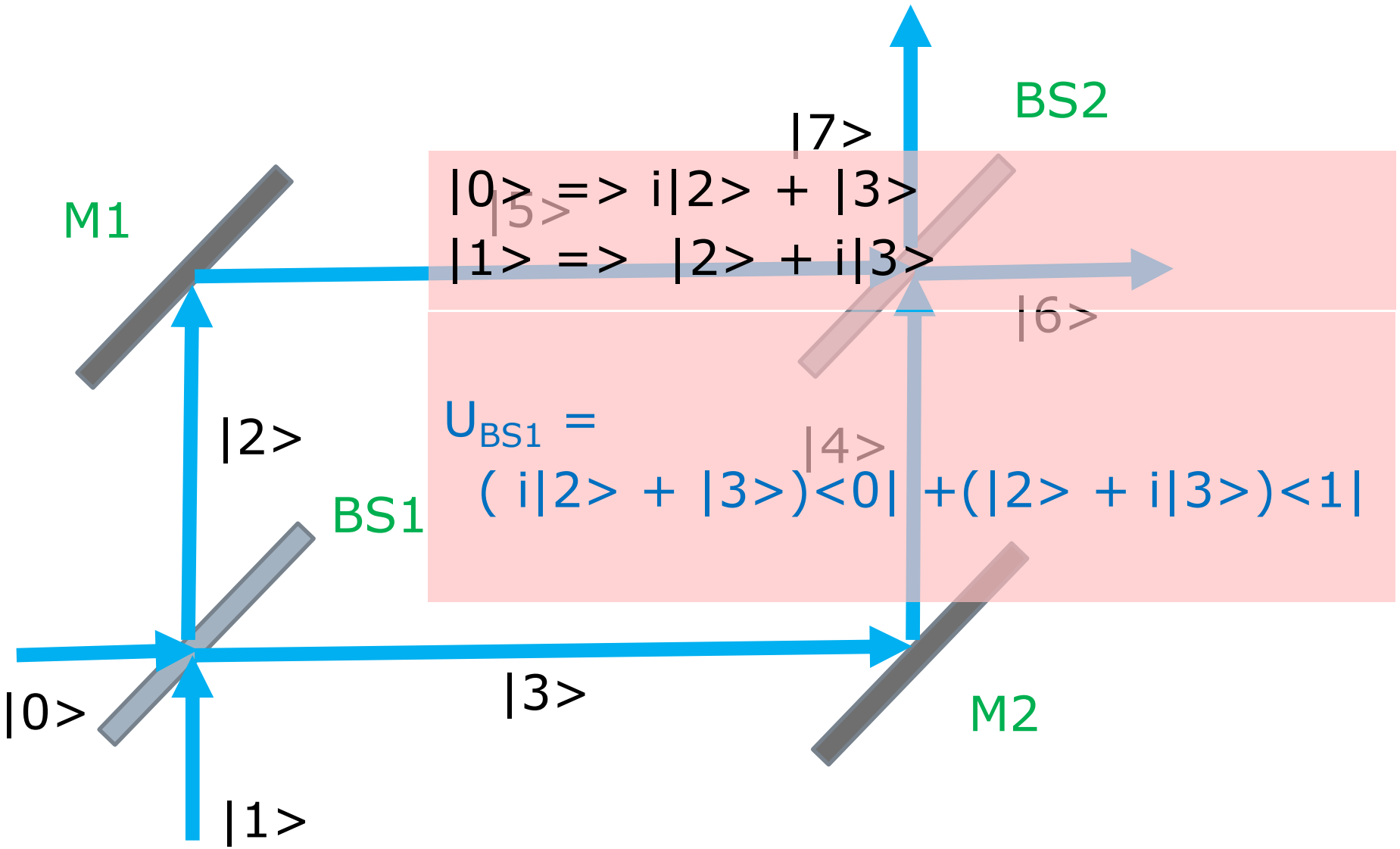
ハーフミラー二つと鏡二つを組み合わせて、上のような装置を作る。光は干渉をおこして、検出器の一方にしか届かなくなる。
奇妙なことは、光子一個で実験しても、このことは変わらない。
一個の光子は、二つの道を「同時」に通っている。

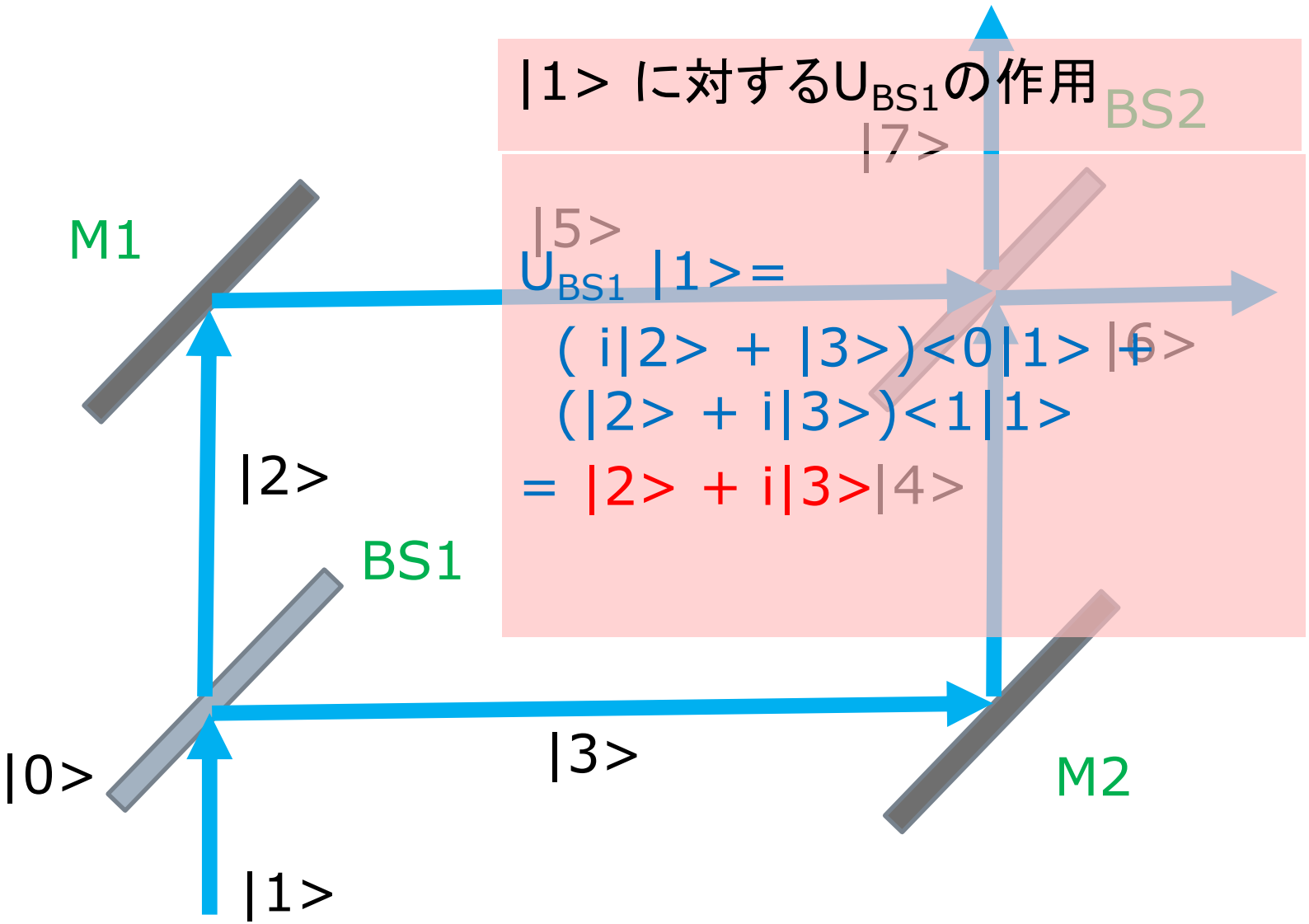


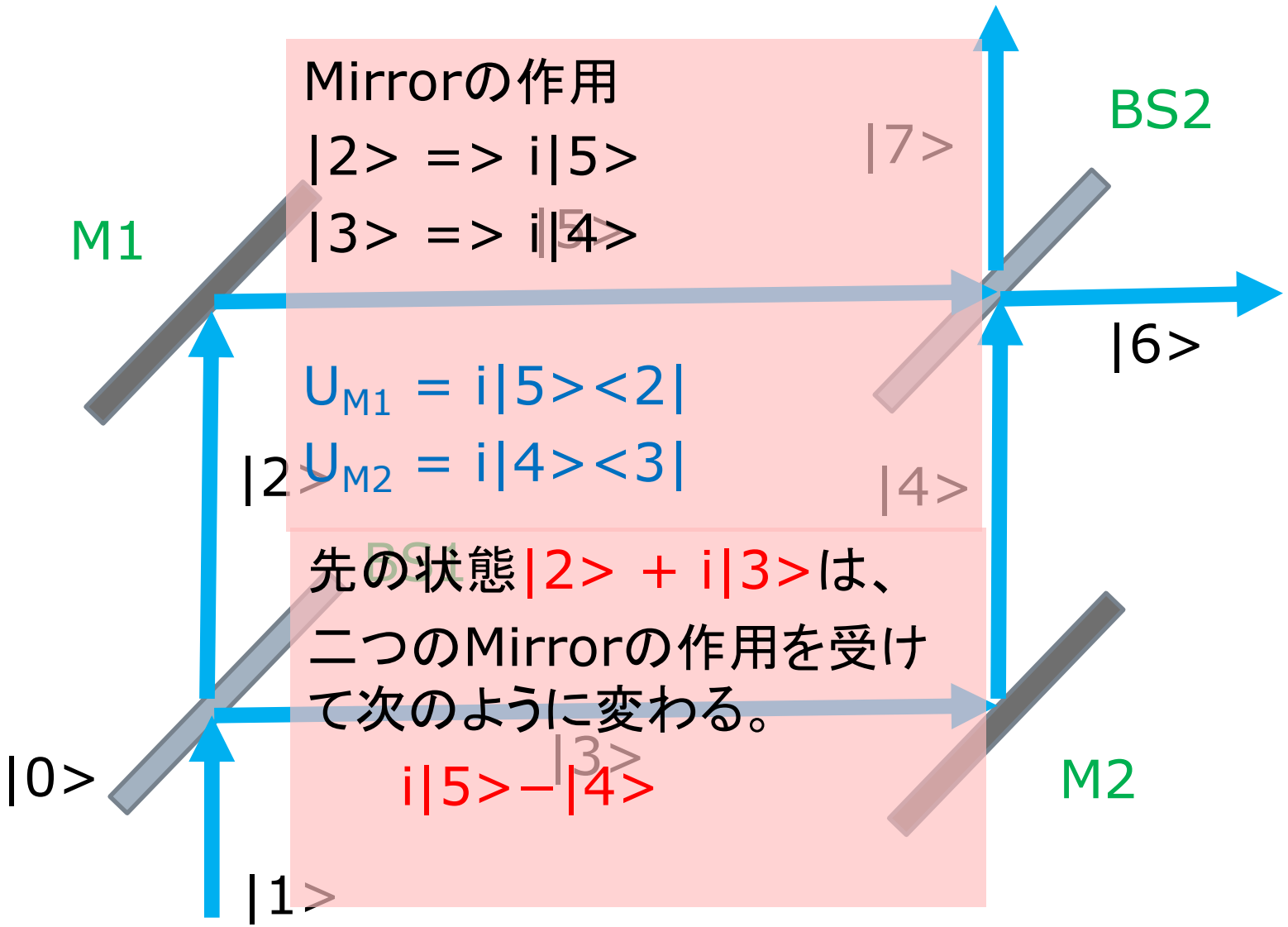
もっと奇妙なことは、光路の一方を塞ぐと、光は両方の検出器に届くようになる。光子一個で考えると、行く手を阻まれた光子は、そのことを、他方の光子に伝えて（どっちも自分自身なのだが）、その性質を変えているように見える。

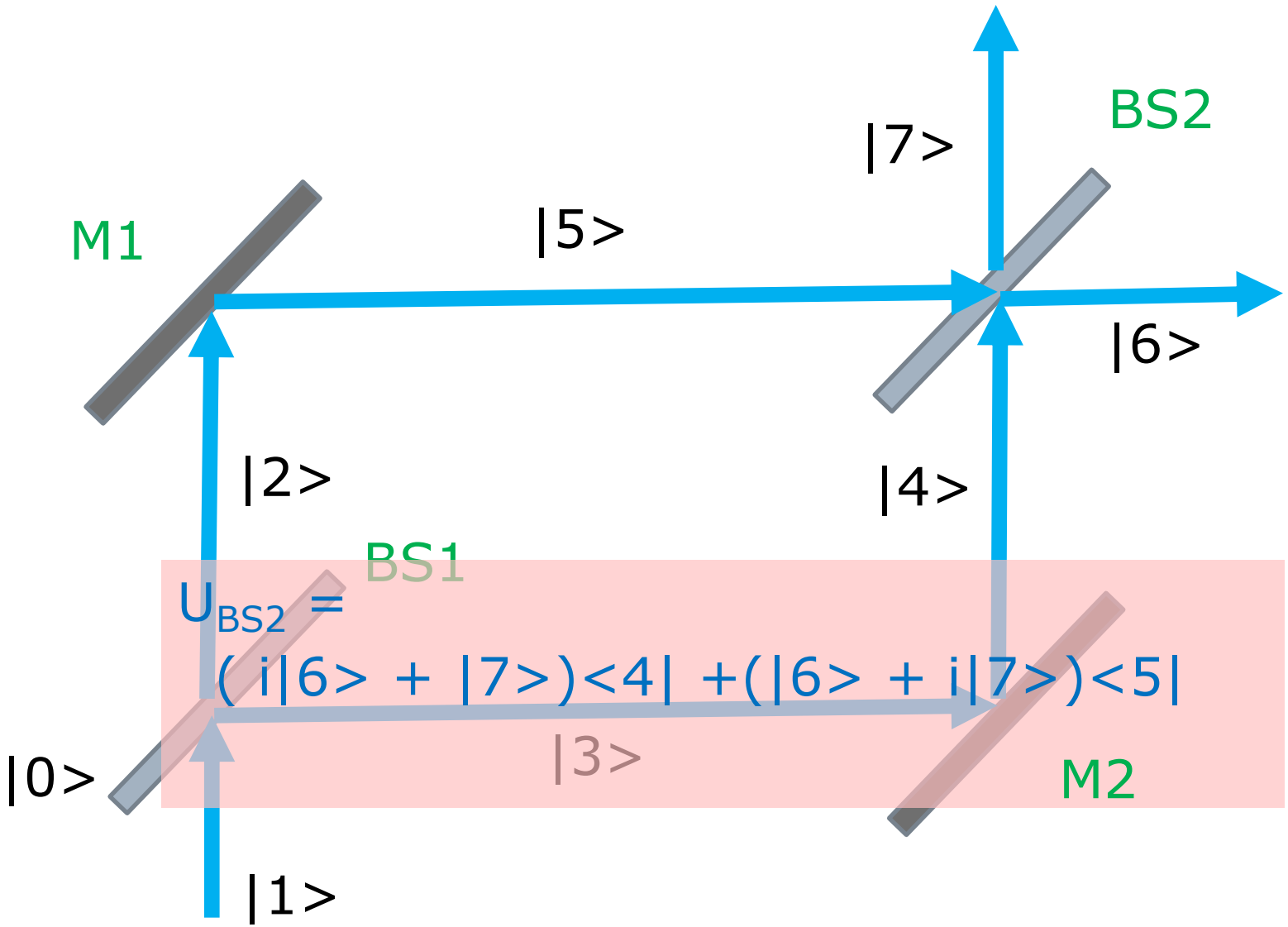
Mach-Zehnder干渉計の働きを計算する

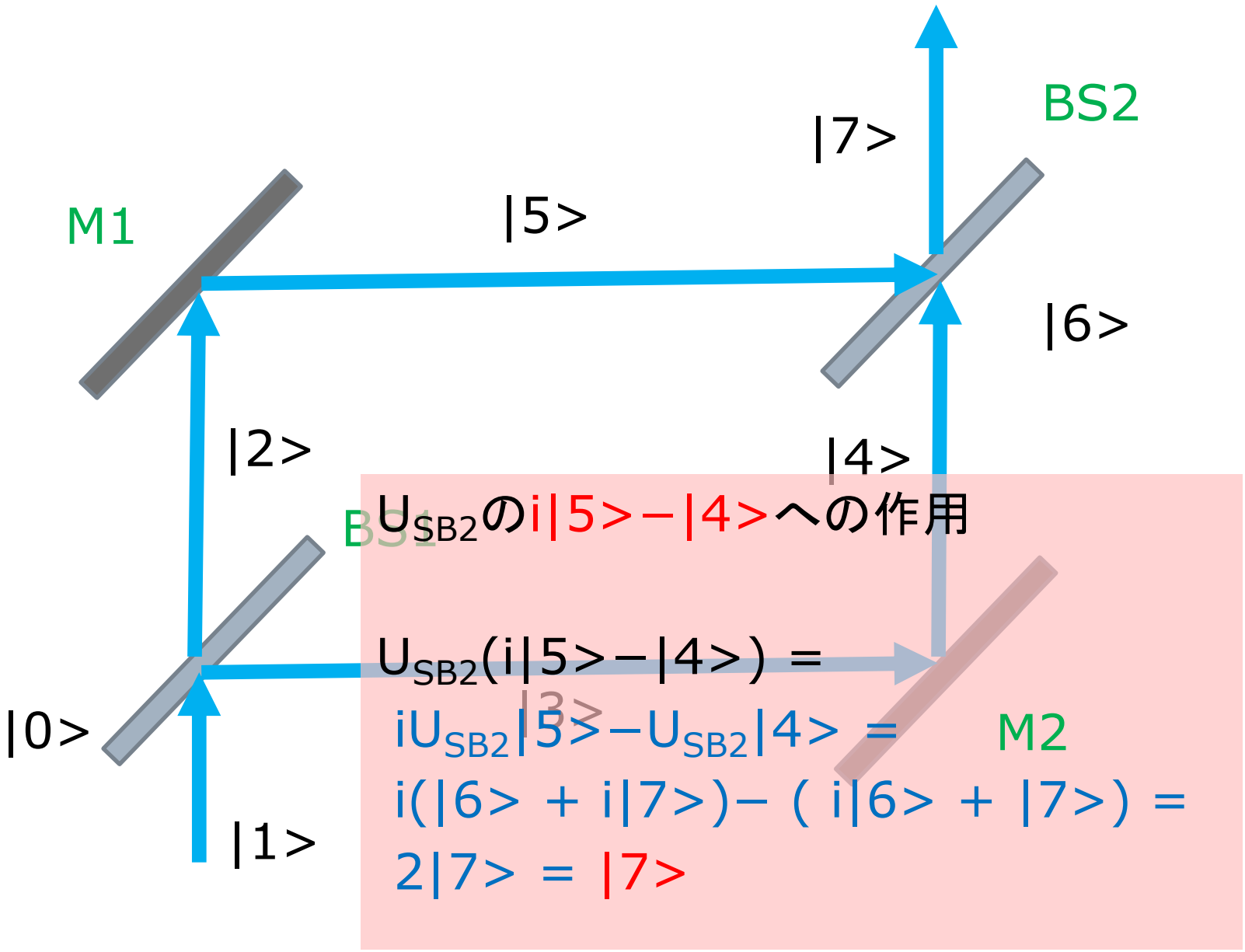

BS2
|7>
M1
|5>
|6>
|2>
|4>
BS1
|0>
|3>
M2
|1>


BS2
|7>
|0> => i|2> + |3>
|1> => |2> + i|3>
M1
|5>
|6>
|2>
U_{BS1} =
|4>
(i|2> + |3>)<0| +(|2> + i|3>)<1|
BS1
|0>
|3>
M2
|1>

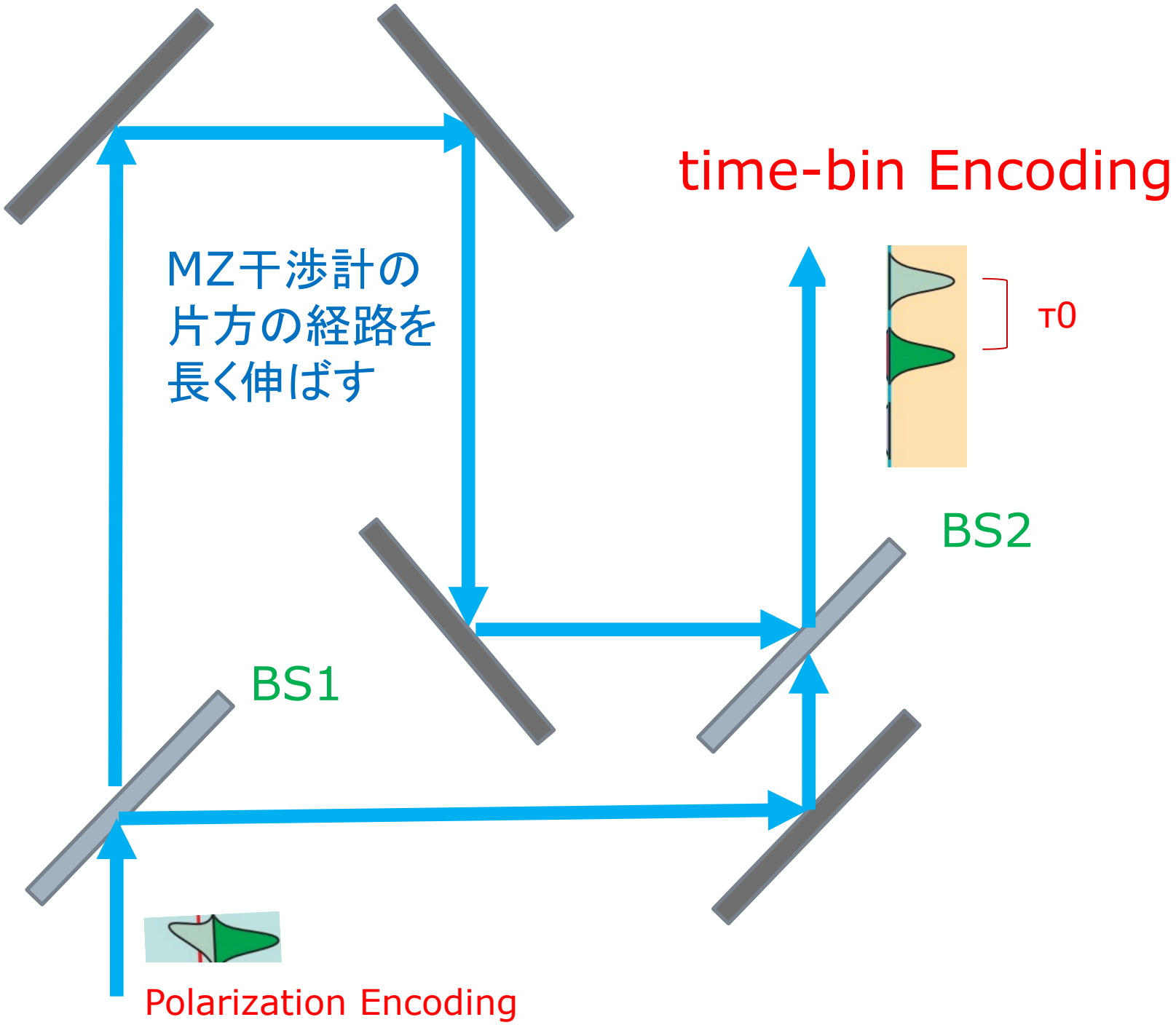

|1> に対するU_BS1の作用
BS2
|7>
M1
|5>
U_BS1 |1>=
(i|2> + |3>)<0|1> |6>
(|2> + i|3>)<1|1>
= |2> + i|3>|4>
|2>
BS1
|0>
|3>
M2
|1>


Mirrorの作用
|2> => i|5>
|3> => i|4>
U_{M1} = i|5><2|
U_{M2} = i|4><3|
先の状態|2> + i|3>は、
二つのMirrorの作用を受けて次のように変わる。
i|5>−|4>
M1
M2
BS2
|0>
|1>
|2>
|3>
|4>
|5>
|6>
|7>


BS2
|7>
M1
|5>
|6>
|2>
|4>
BS1
U_{BS2} =
(i|6> + |7>)<4| +(|6> + i|7>)<5|
|3>
|0>
M2
|1>

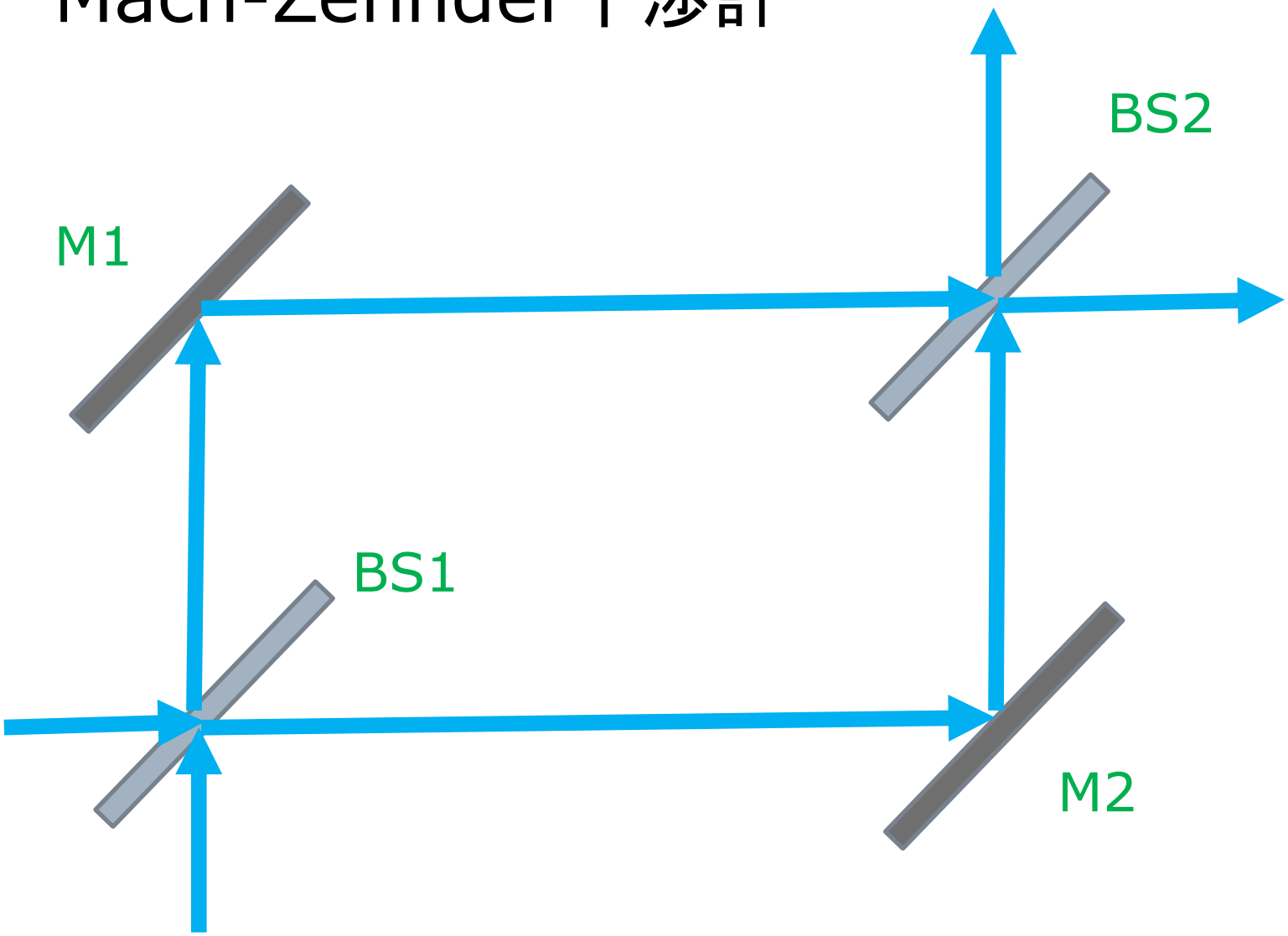

M1
BS2
|7>
|5>
|6>
|2>
|4>
BS1
|3>
|0>
|1>
M2
U_{SB2}のi|5>−|4>への作用
$U_{SB2}(i|5\rangle-|4\rangle)$ =
$iU_{SB2}|5\rangle-U_{SB2}|4\rangle$ =
i(|6> + i|7>)− (i|6> + |7>) =
2|7> = |7>

time-bin qubit encoding

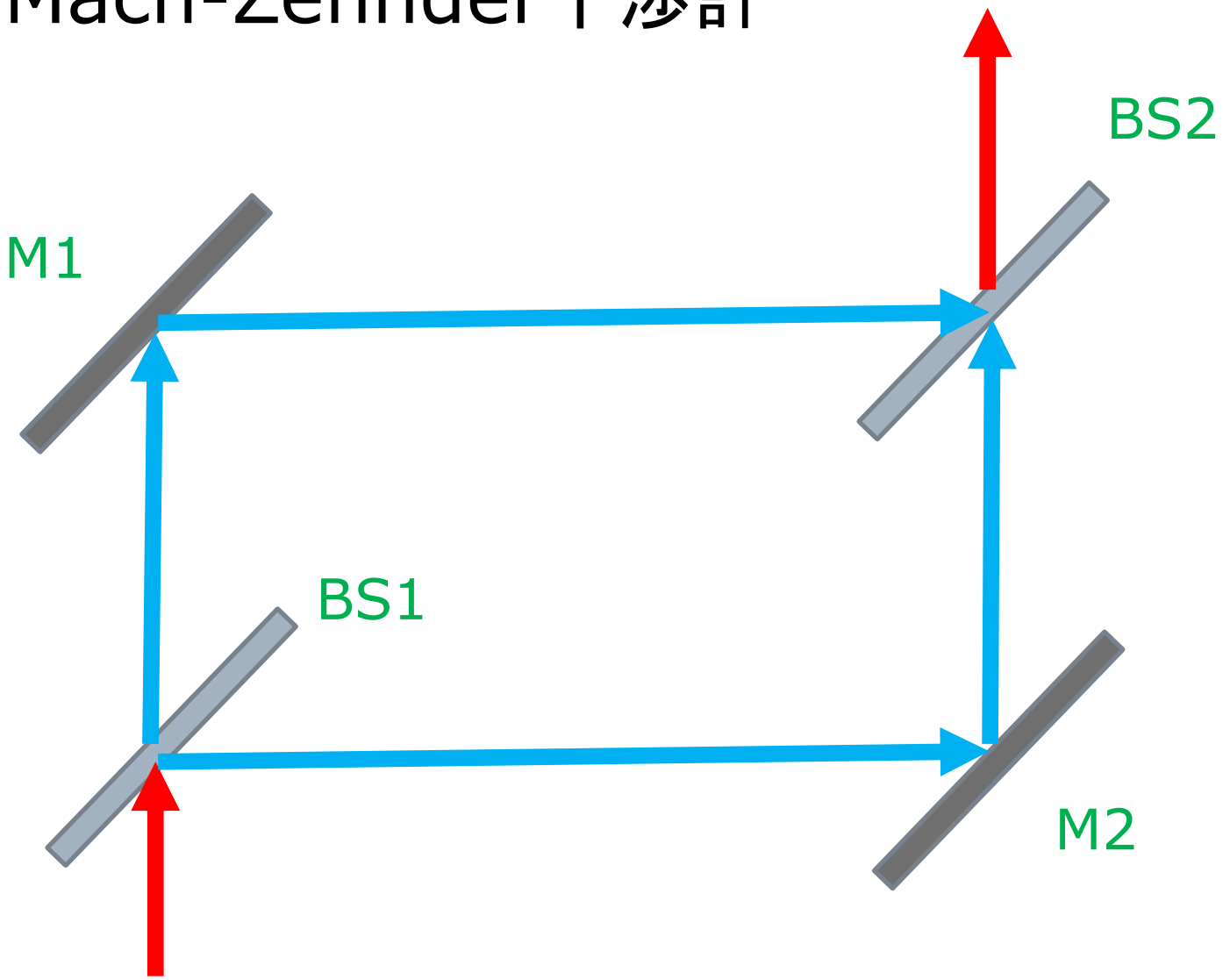

time-bin Encoding
MZ干渉計の
片方の経路を
長く伸ばす
τ0
BS2
BS1
Polarization Encoding

time-bin qubit encoding 回路の形

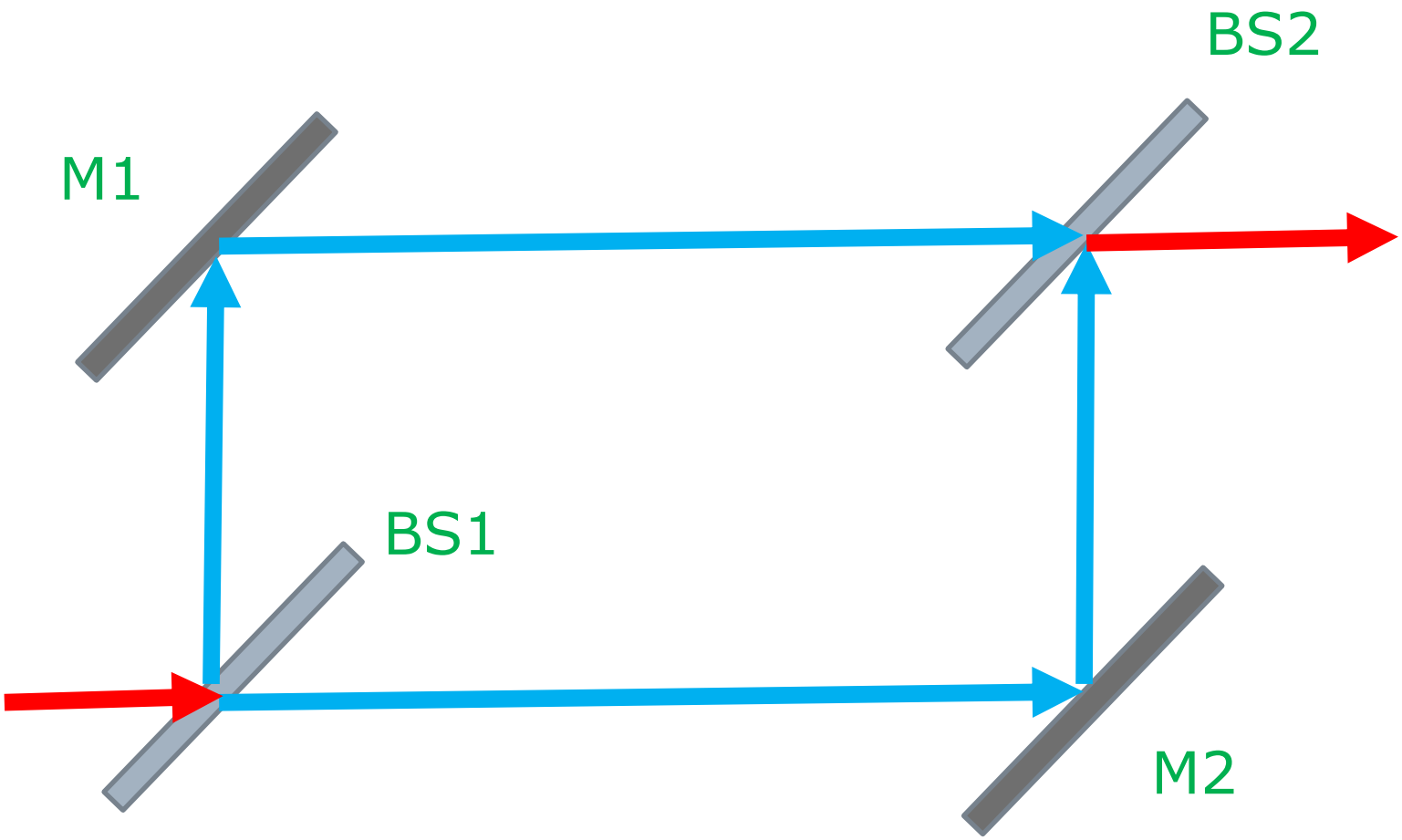
Mach-Zehnder干渉計

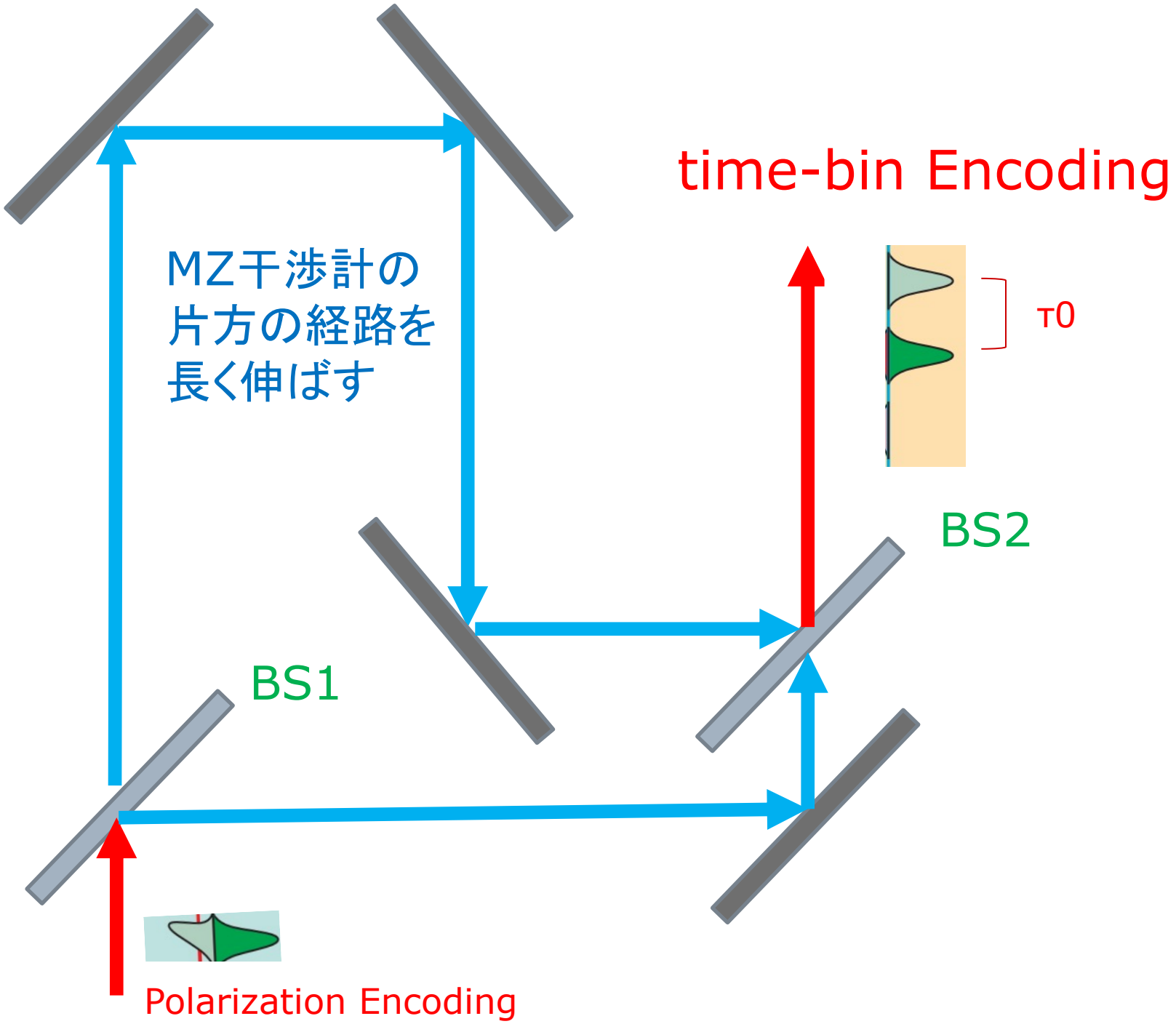


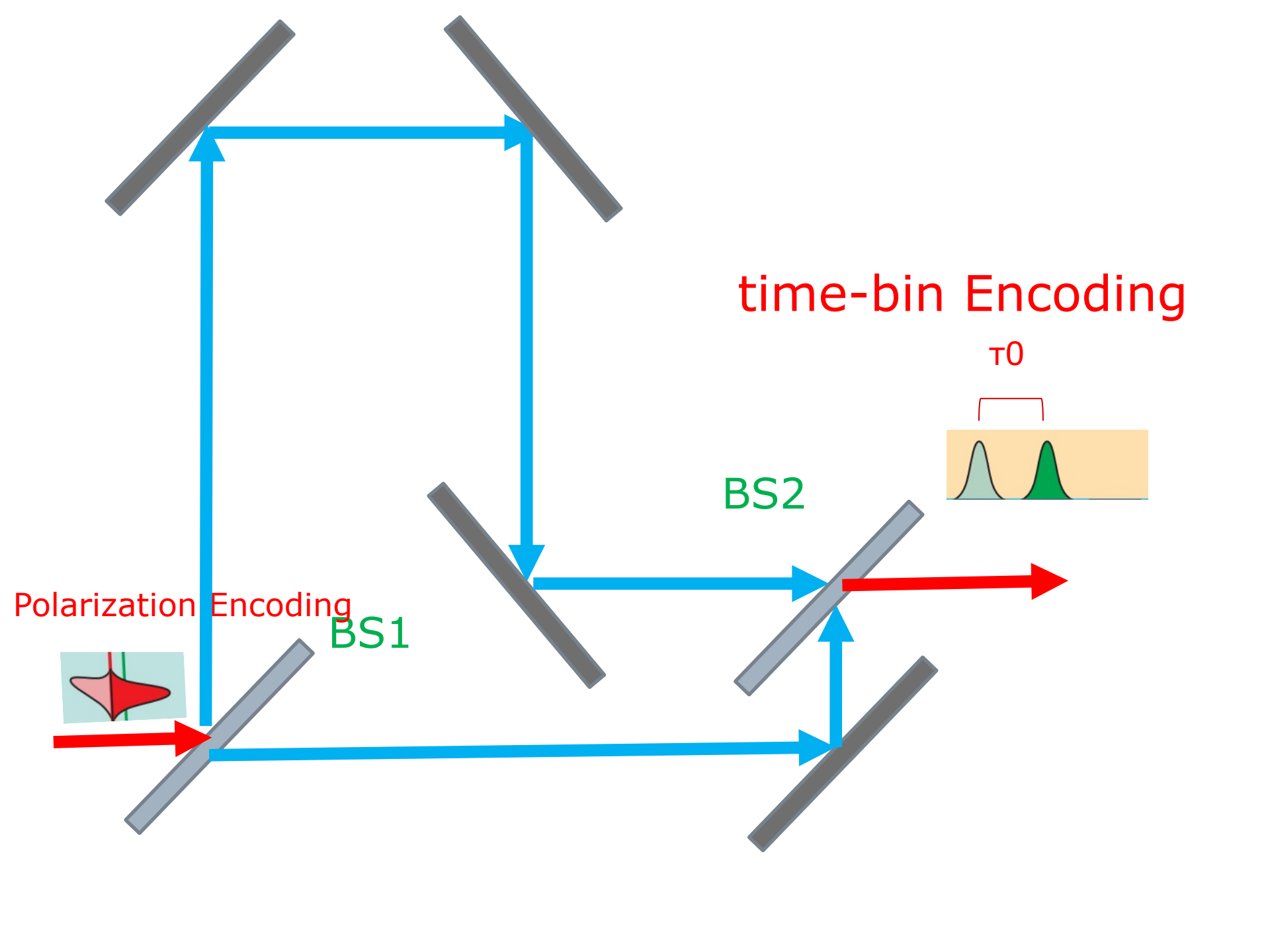
Mach-Zehnder干渉計

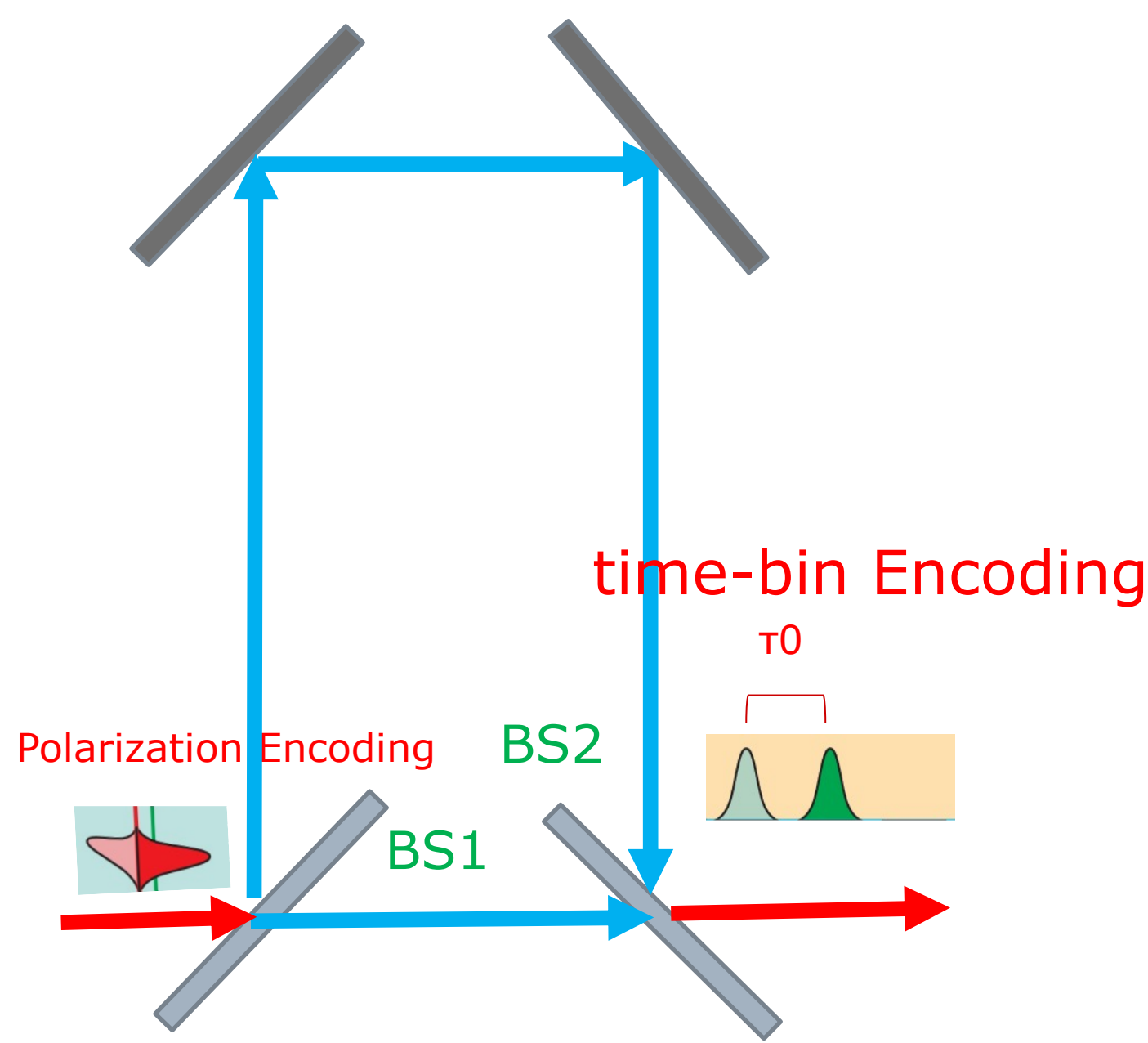


Mach-Zehnder干渉計

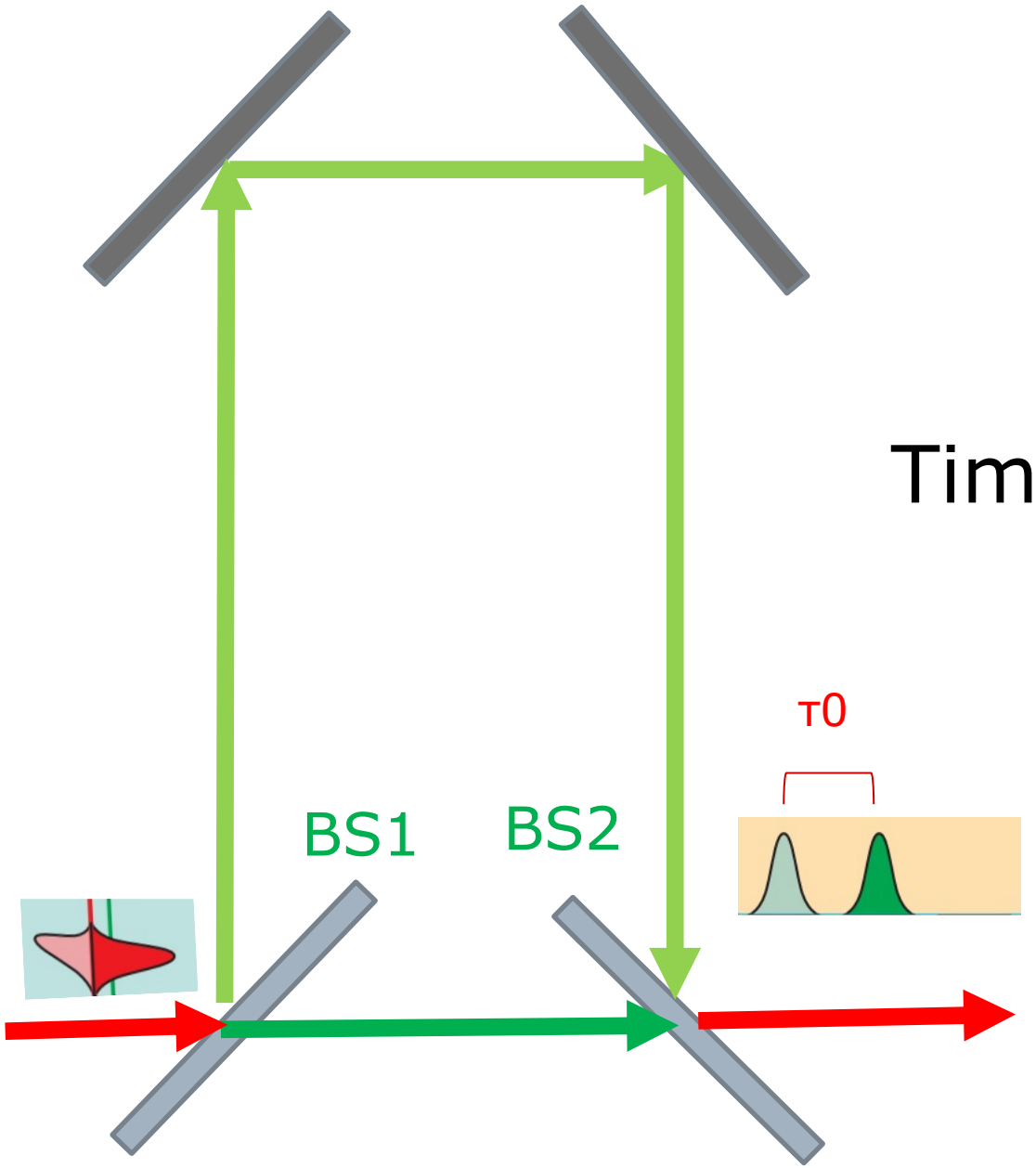



time-bin Encoding
MZ干渉計の
片方の経路を
長く伸ばす
τ0
BS2
BS1
Polarization Encoding


time-bin Encoding
τ0
BS2
Polarization Encoding
BS1


time-bin Encoding
τ0
Polarization Encoding
BS2
BS1

Time-bin Encoder



Entangleしたsingle photonペアの time-bin encodingの実験

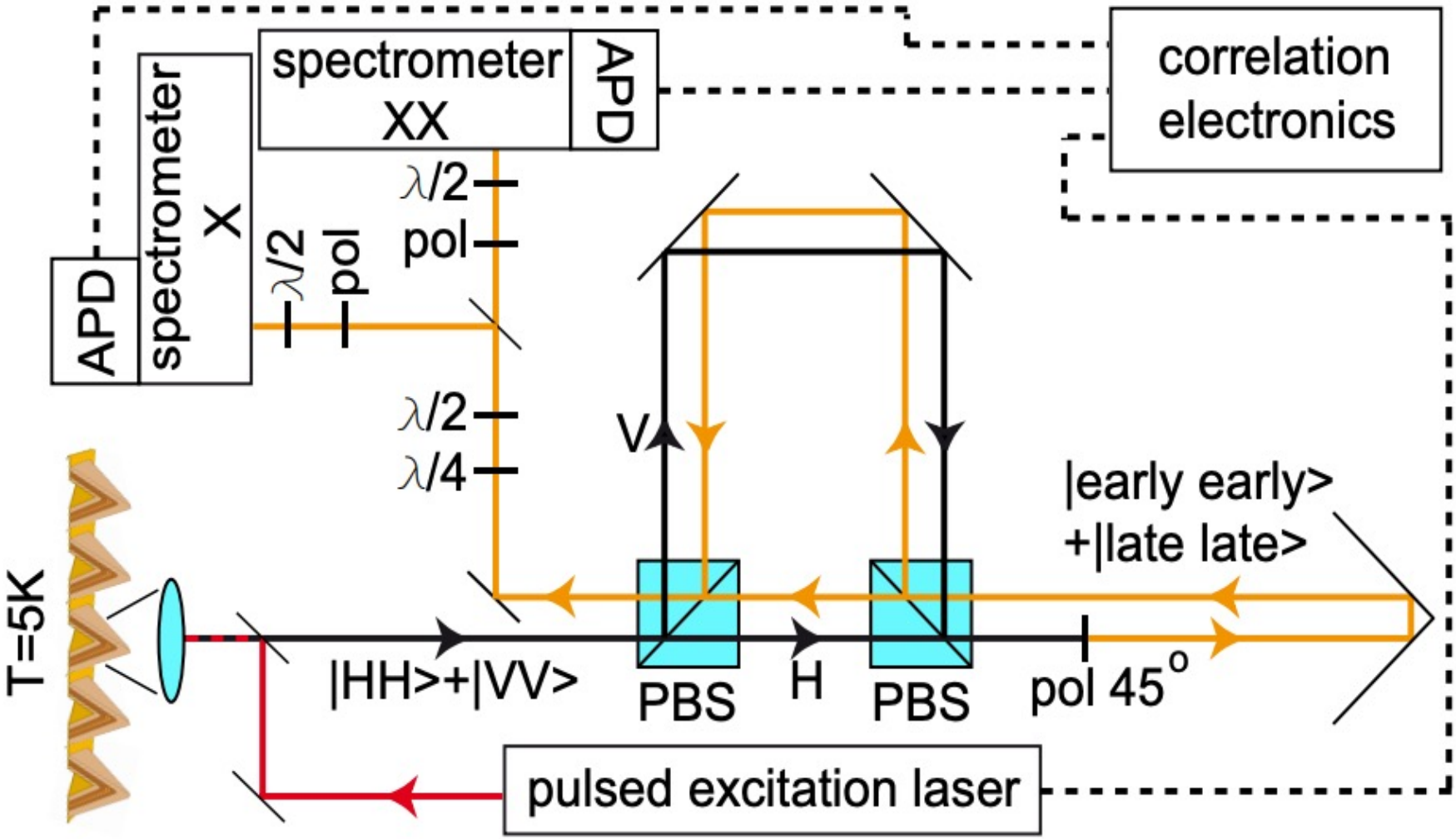
time-bin encoding の EntangleしたphotonペアへのEntangleしたphotonペアへの応用

今回は、time-bin encodingの手法が、エンタングルしたphotonのペアにも有効であることを示した初期の実験を紹介しようと思う。

前回見た、time-bin encoding の回路の働きを見るのにも、ちょうどいいと思う。

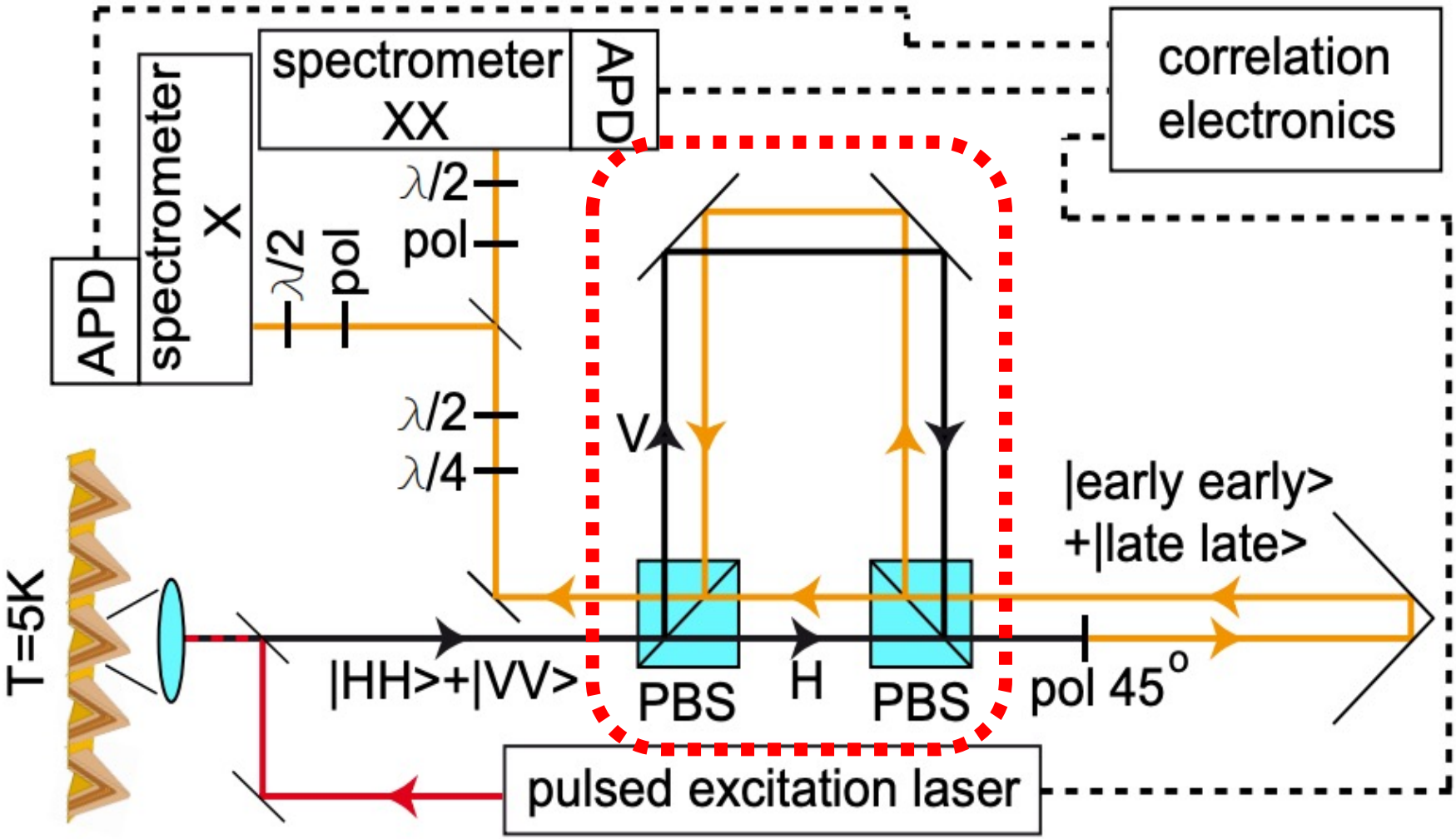
ただし、この回路は実用的なものではない。今日では、こうした実験をベースに、大きな前進が見られる。

Single pairs of time-bin entangled photons



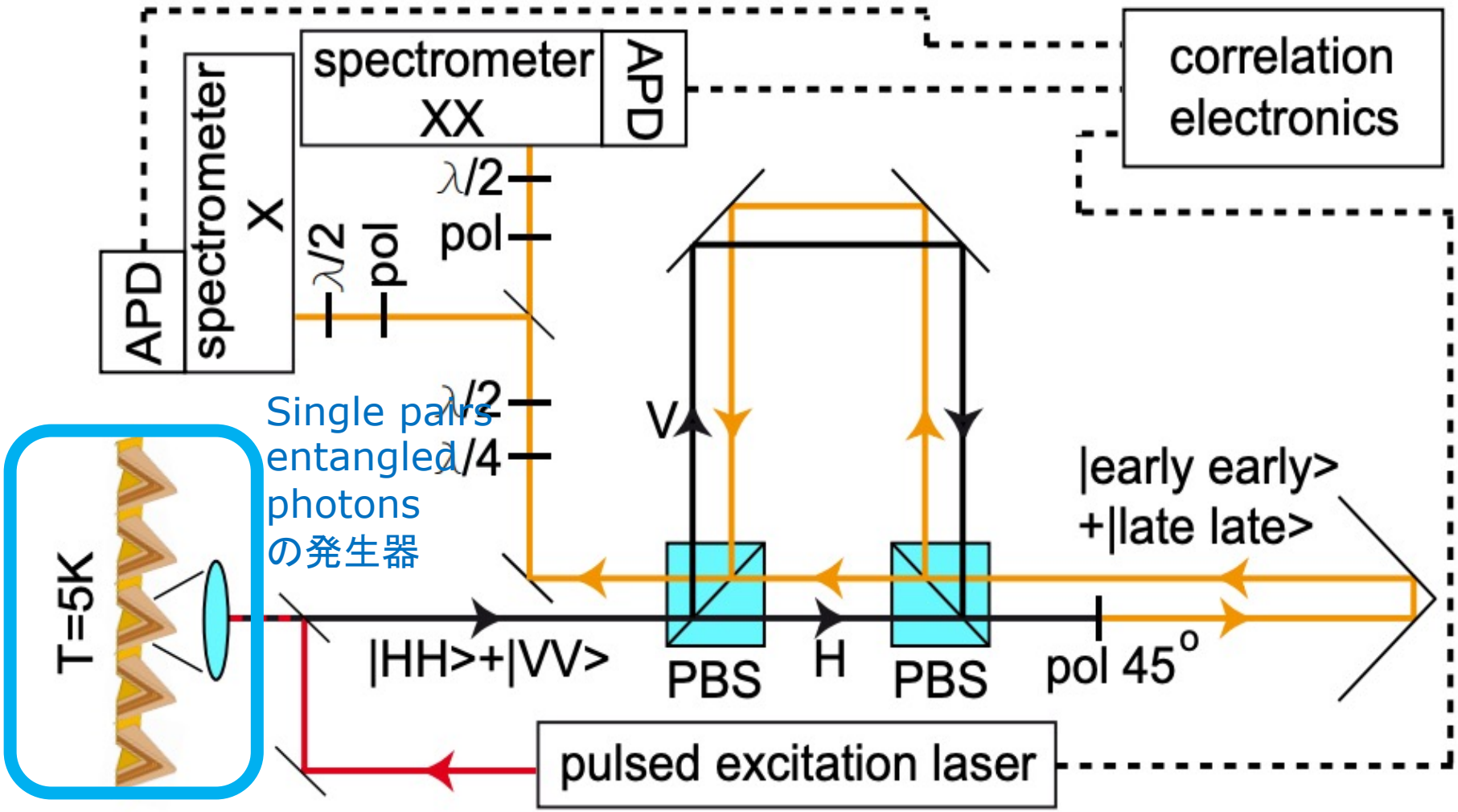
https://arxiv.org/pdf/1507.01876.pdf

Single pairs of time-bin entangled photons



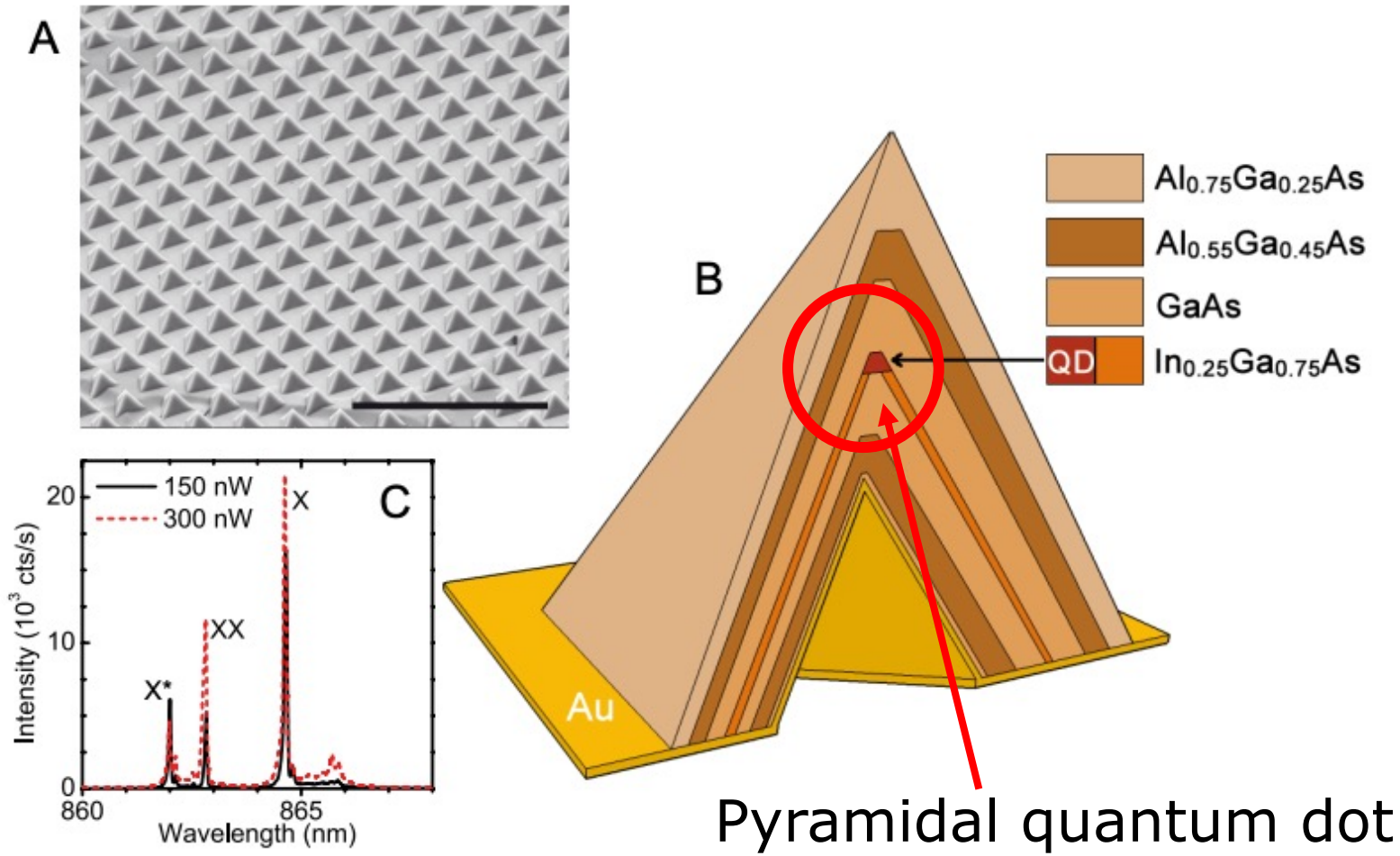
https://arxiv.org/pdf/1507.01876.pdf

Single pairs of time-bin entangled photons



https://arxiv.org/pdf/1507.01876.pdf

Single pairs entangled photonsの発生器



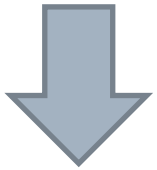
Polarization Encodingから Time-bin Encodingへ

Single pairs entangled photonsの発生器は、entangleしたXXとXの2個のphotonのペアを一つ生成する。

Polarization Encoding

|HH> + |VV>　H:Horizontal　V:Vertical

先がXXの状態、後ろがXの状態



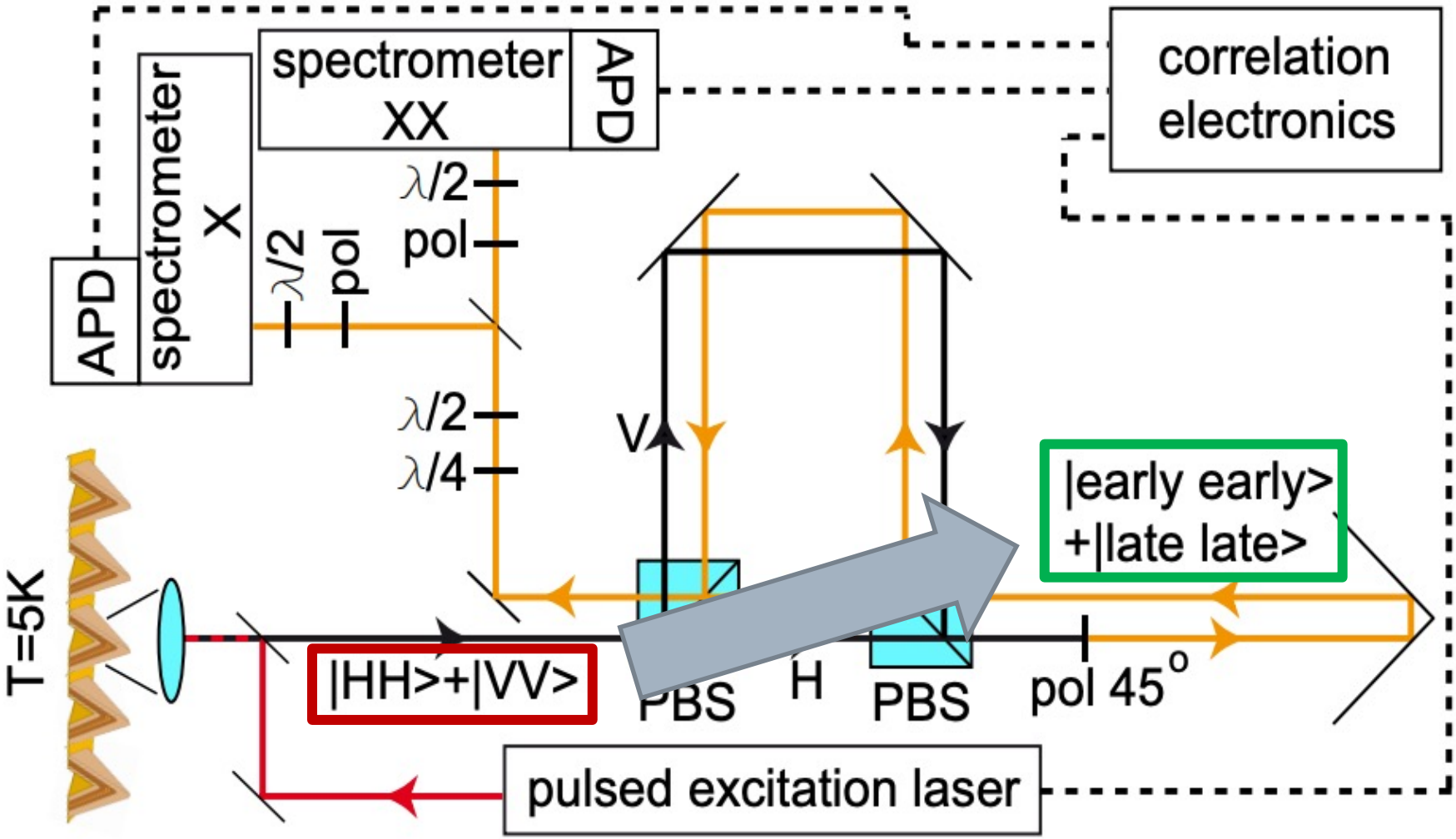
Time-bin Encodeing

|early early> + |late late>

early: 先着のパルス　late: 後着のパルス

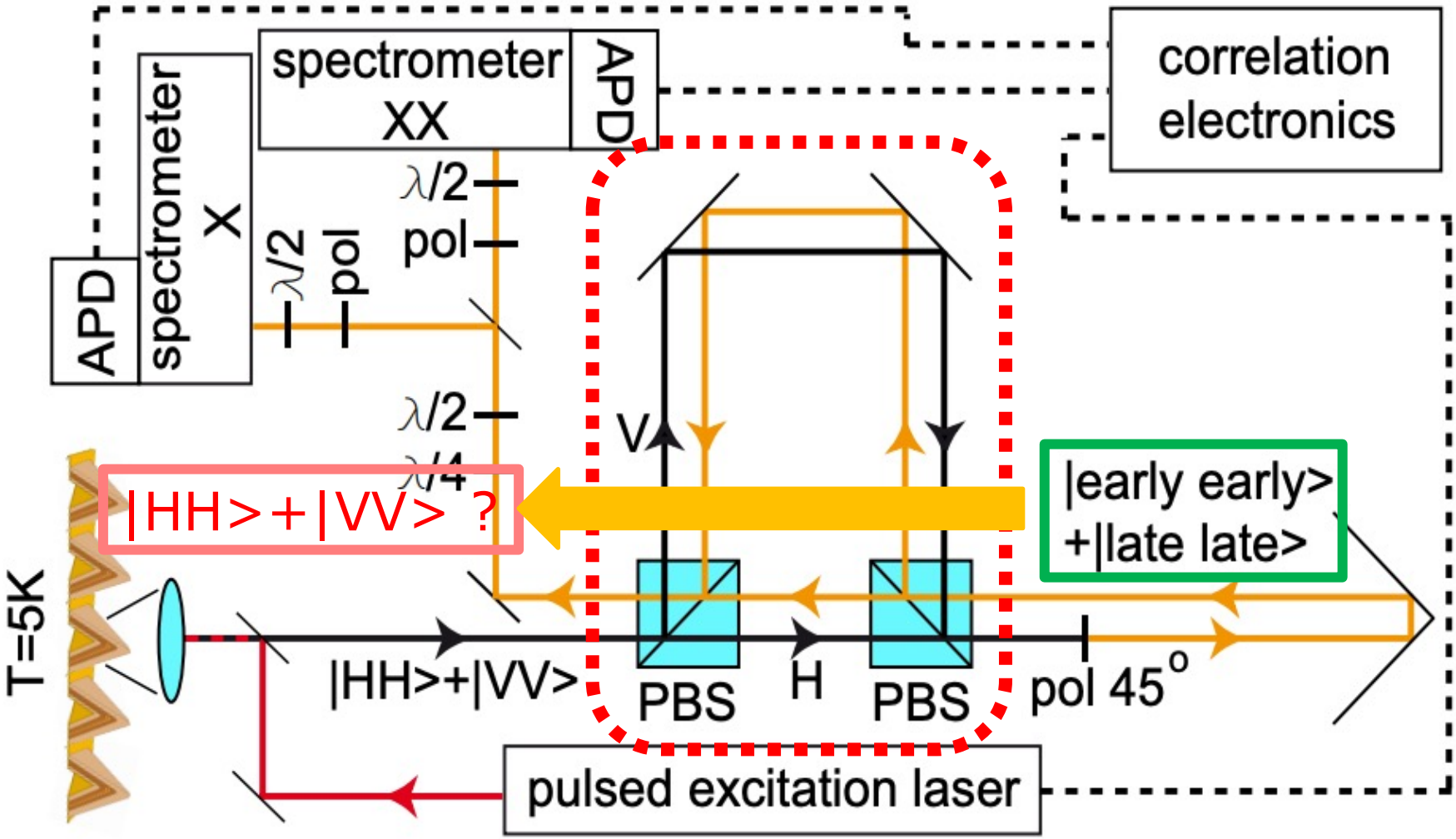
先がXXの状態、後ろがXの状態

Single pairs of time-bin entangled photons



https://arxiv.org/pdf/1507.01876.pdf

Single pairs of time-bin entangled photons



https://arxiv.org/pdf/1507.01876.pdf