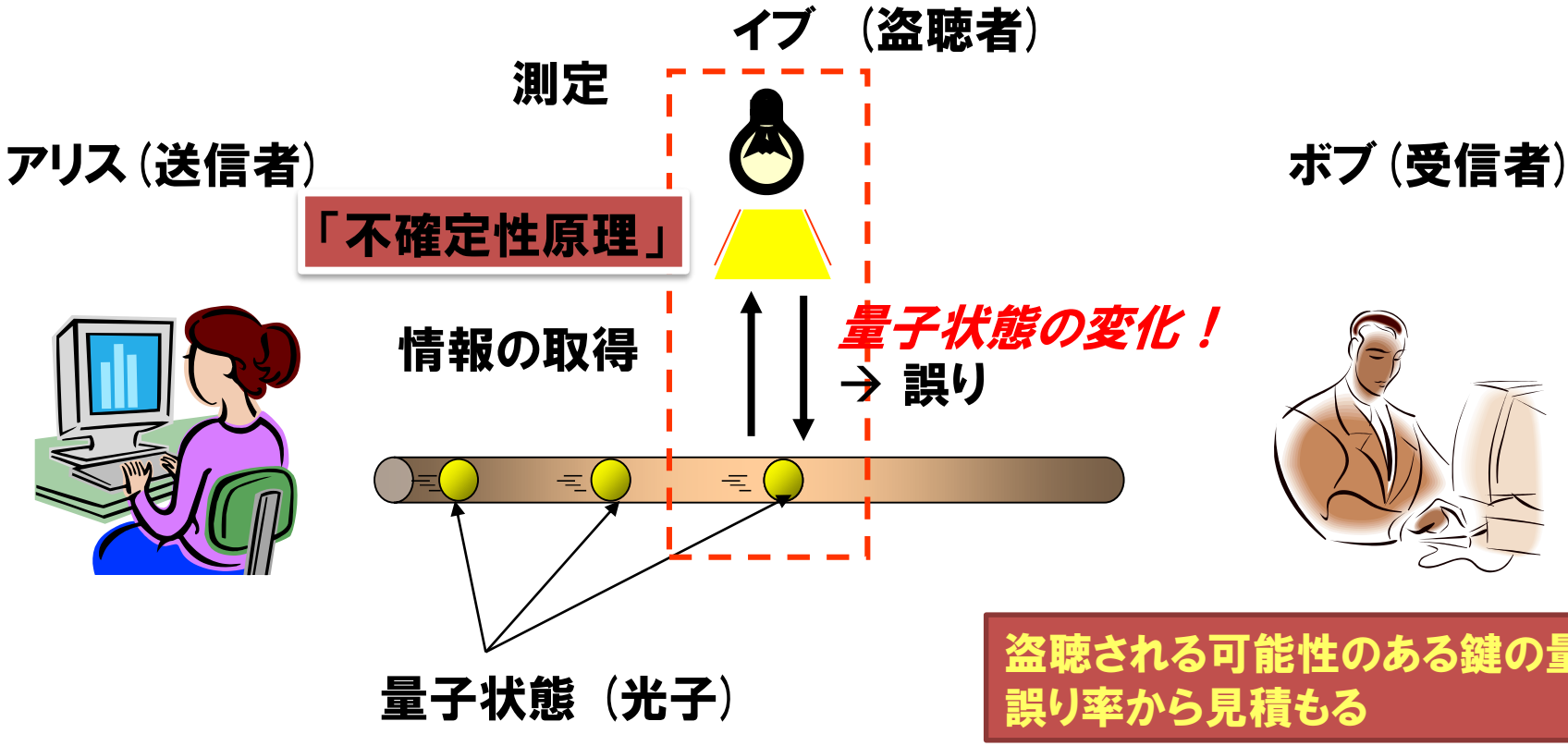
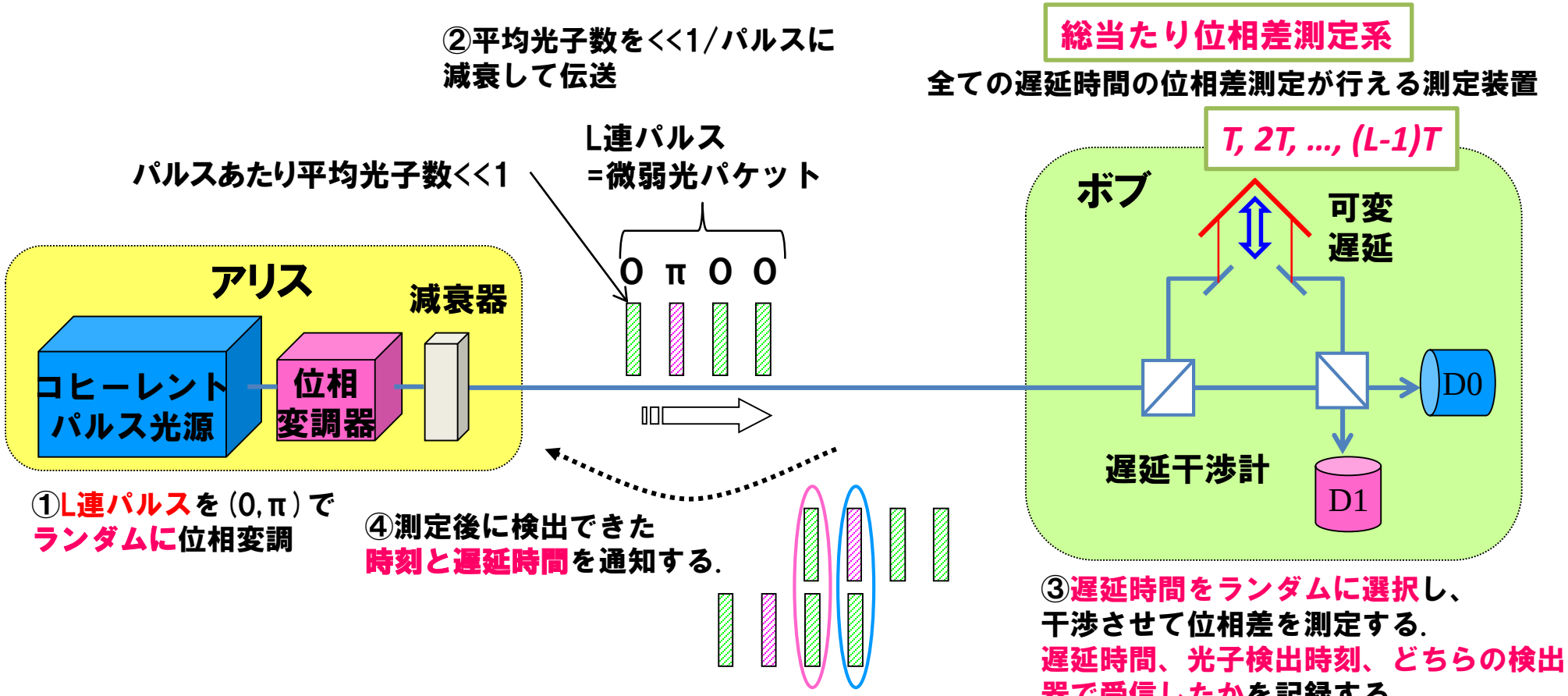
図1：従来の量子鍵配送（QKD）

QKD: 暗号通信のための「鍵」を離れた2者間で安全に共有する



従来のQKD：不確定性原理を利用したQKD→盗聴すると誤りが出る

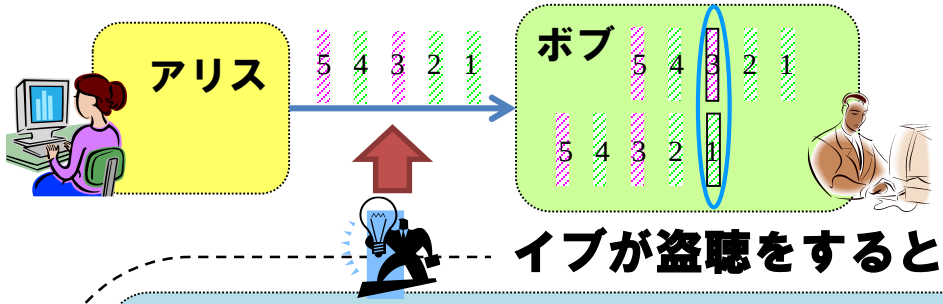
図2：RRDPS方式



⑤検出時刻と遅延時間よりアリスはボブがどちらの検出器で受信したかがわかる→秘密鍵

図3: RRDPS方式はなぜ安全か

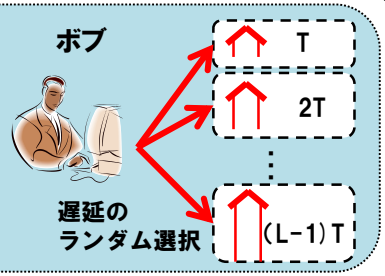
RRDPS：測定における波束（量子状態）の収縮を利用したQKD→そもそも読めない



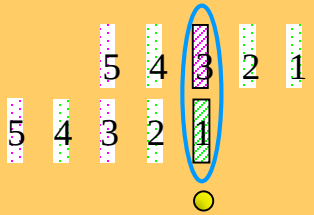
アリスは、ボブが読み出しに成功した
2パルス間の位相差を採用する。

イブが盗聴をするとき

ボブがどの遅延時間の位相差の読み出しに成功するかは、
(L−1) 個の中からランダムに選んだ遅延時間に依存するので、
イブは制御できない



アリスから送り出されるL連パルスのどのパルスで光子が
測定されるかはランダムなので、イブは特定の
2パルス間の位相差を狙って読み出すことはできない



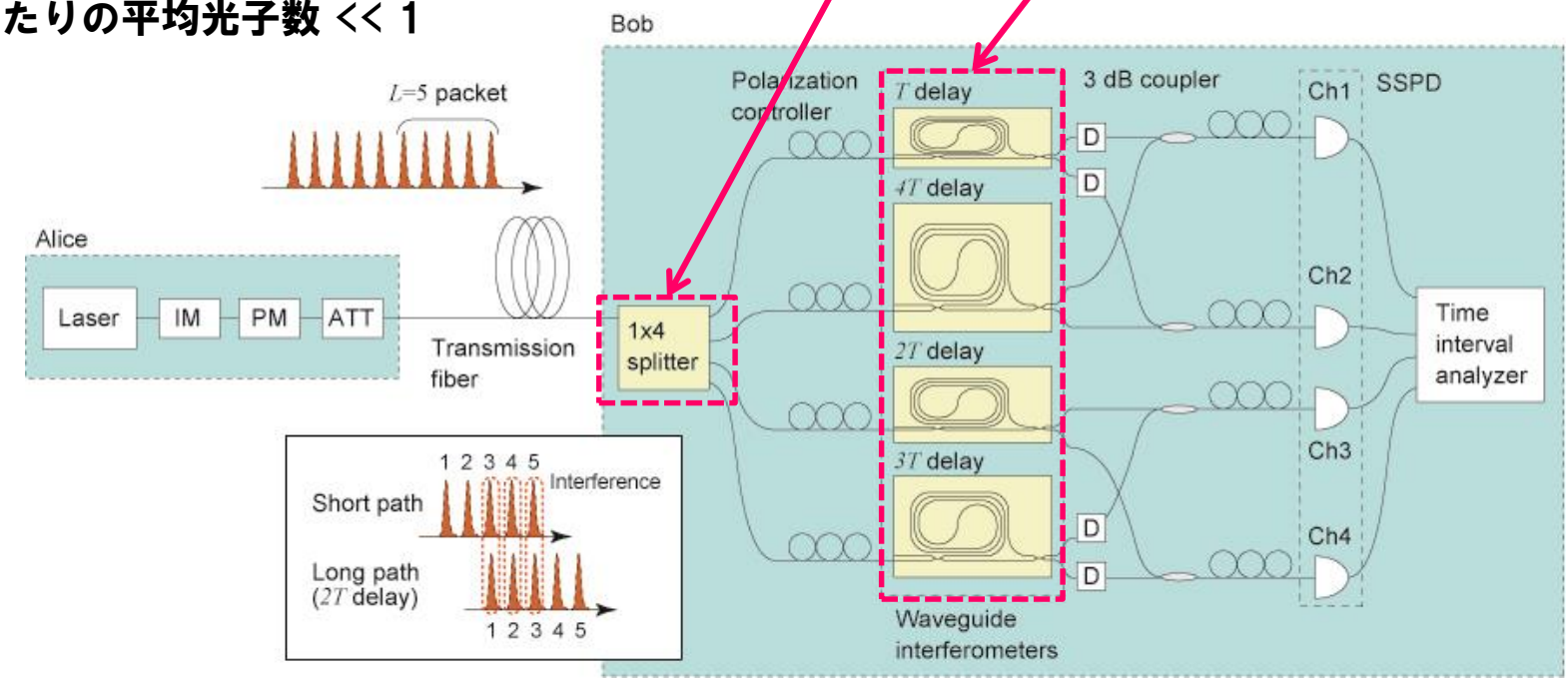
イブの盗聴は、自分が位相差を読み出した2パルスが
偶然ボブと一致したときに成功する
この偶然の確率はパルス数Lのみにより依存し、誤り率に無関係

図4：総当たり位相差測定の実装

クロック周波数: 2 GHz
パルス数L=5のパケット
パルスあたりの平均光子数 << 1

1x4光スプリッタ：光子の経路をランダムに選択

T～4Tの遅延干渉計

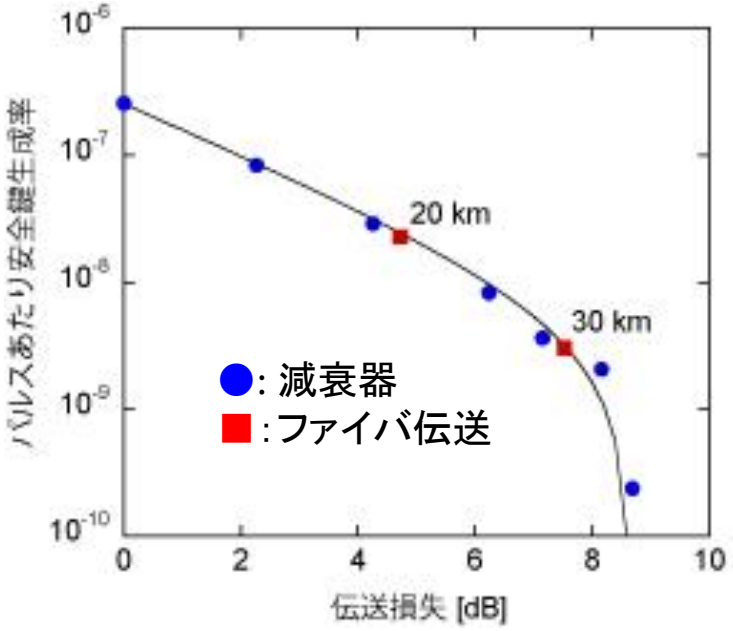


受動素子を用いてT～4Tの遅延干渉計をランダムに選択する仕組みを実装

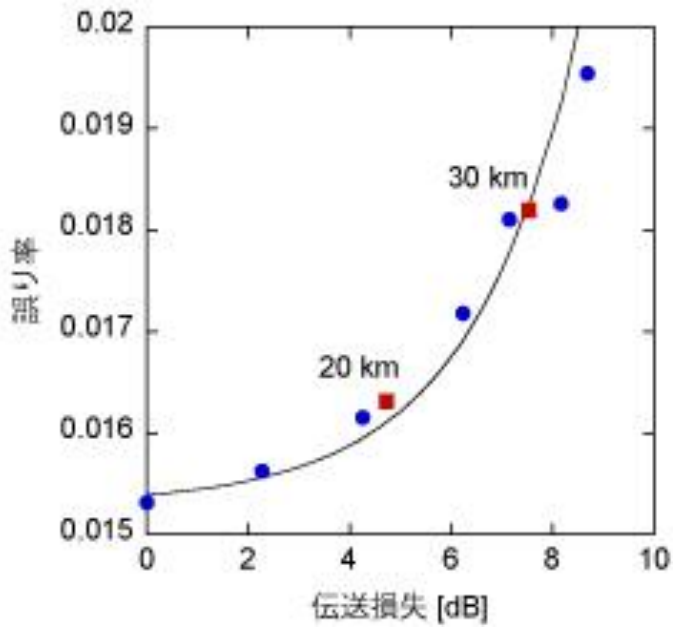
→　低損失、高い位相安定度

図5：鍵配送実験結果

安全鍵生成率と伝送損失の関係



誤り率と伝送損失の関係



RRDPSプロトコルの原理確認実験に成功（安全鍵生成を初めて実現）
性能：30 kmのファイバ伝送を達成。最大伝送損失は～9 dB。

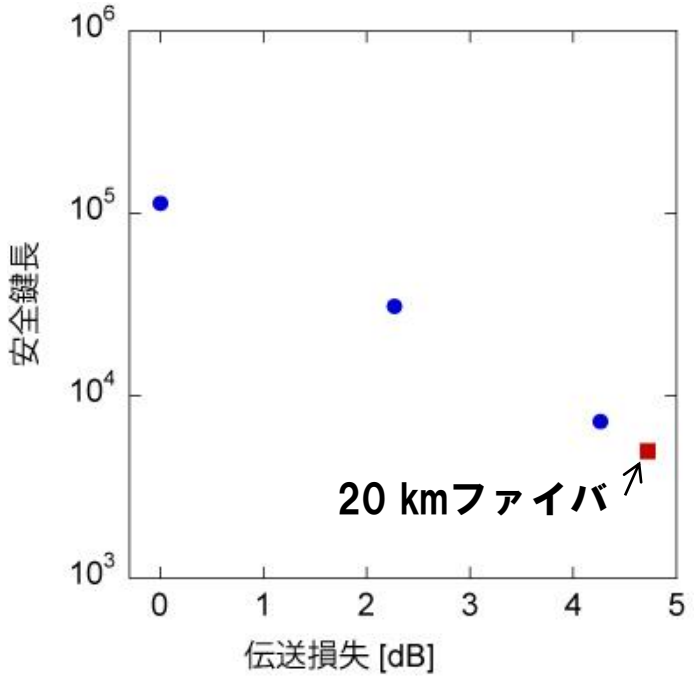
※鍵の長さの有限性による情報漏洩量の揺らぎを考慮に入れない安全性評価

図6：鍵の長さの有限性を考慮した安全性解析

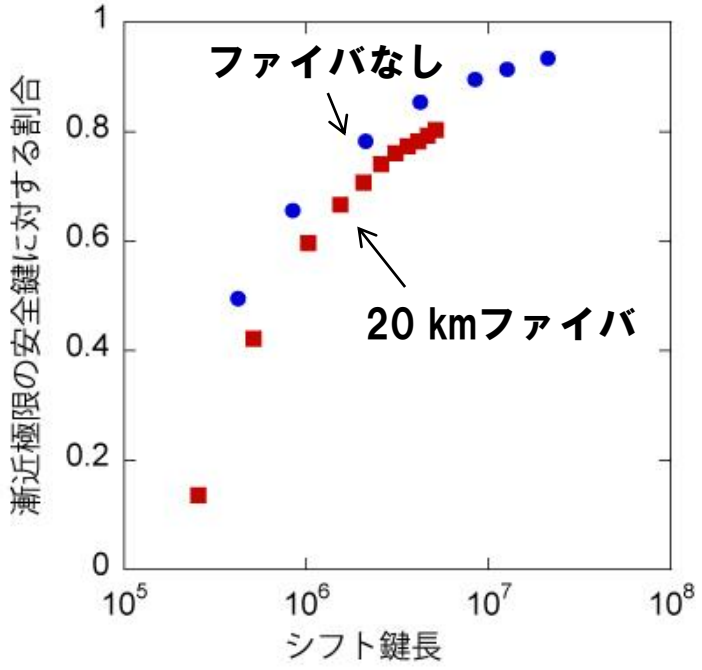
現実のQKDシステムでは必ず鍵の長さは有限　→　情報漏洩量見積もりの揺らぎ（安全鍵生成に「失敗」する可能性）

鍵の長さの有限性を考慮しても安全な鍵の長さを計算した

有限長を考慮した安全鍵長と伝送損失の関係
（測定時間を260 sに固定）



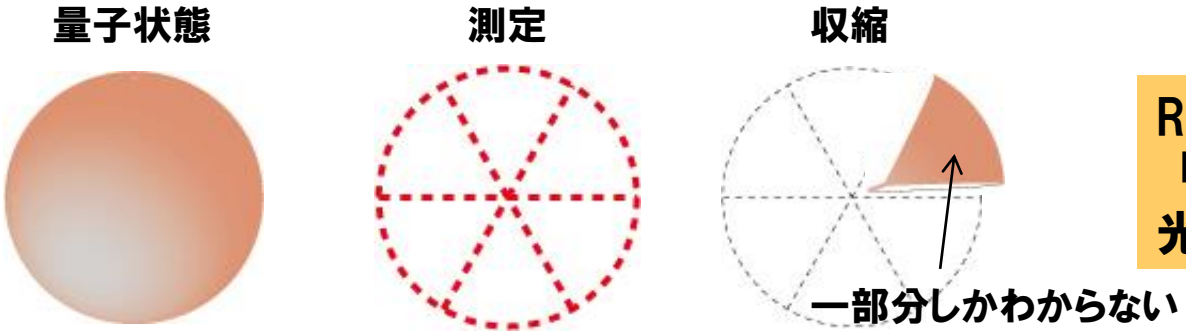
有限長を考慮に入れない安全鍵に対する割合



鍵の長さの有限性を考慮した現実のシステムでも
安全な鍵配送が可能であることを確認

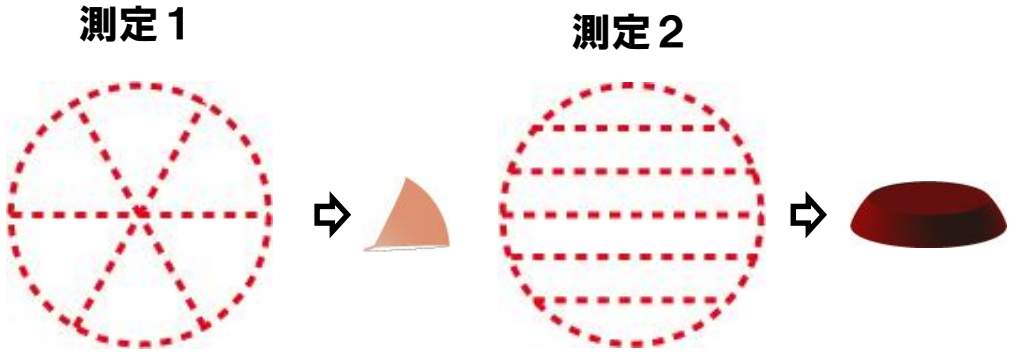
図7：波束の収縮

1．波束の収縮とは、測定前は（たとえば光子の場所が）定まっていない量子状態（波束）が、
測定によって「収縮」して光子の場所が決まるという性質。測定すると、一部分しかわからない



RRDPS方式では、
「どれか一つのパルスでのみ
光子が観測される」ことに相当

2．どのように量子状態を「切るか」は測定する人が選べる



RRDPS方式では、
「ボブが遅延時間をランダムに
選択する」ことに相当