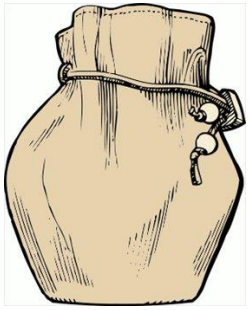
Quantum Entanglement, and Applications

Brad Christensen

Advisor: **Paul G. Kwiat**



Physics 403 talk: April 24, 2013

Entanglement is a feature of compound quantum systems

- States that can be written $|\Psi\rangle_{AB} = |\varphi^1\rangle_A |\varphi^2\rangle_B$ are separable
- States that cannot be written this way are entangled

Example: the *Bell states* are inseparable

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle)$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)$$

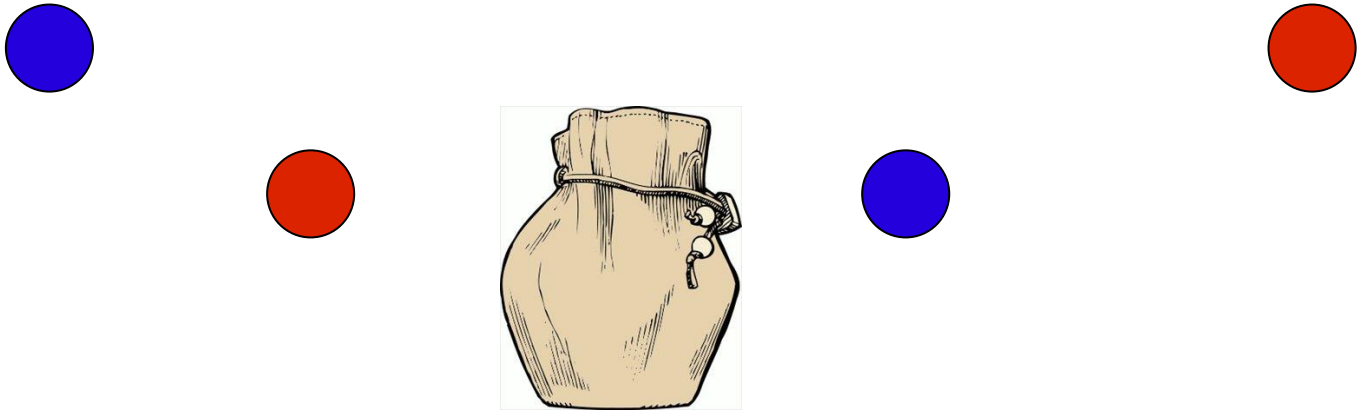
$$\begin{aligned}|\Phi'\rangle &= (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) \\ &= \alpha\gamma|0\rangle|0\rangle + \alpha\delta|0\rangle|1\rangle + \beta\gamma|1\rangle|0\rangle + \beta\delta|1\rangle|1\rangle\end{aligned}$$

No solution!

Measurement outcomes are random and correlated

Classical “entanglement”?

- Classical things can be random and correlated, too…



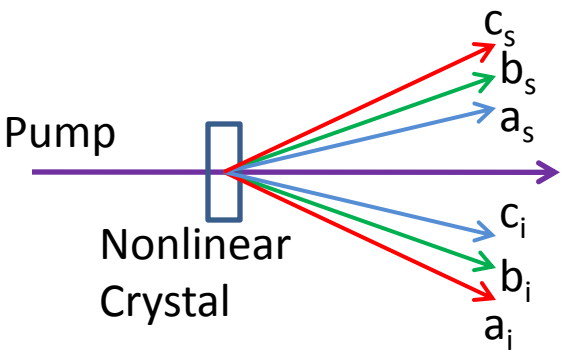
- … but not entangled!

How is this different from an entangled state?

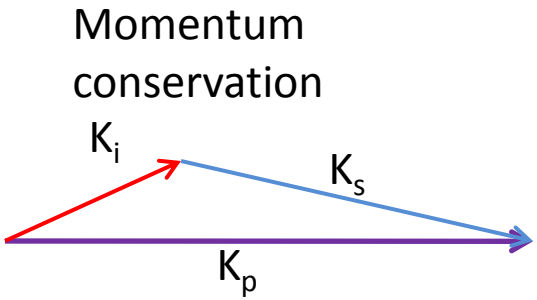
- Each marble has a defined color from the beginning (local hidden variable)
- The processes are distinguishable in principle
- There is no conjugate measurement basis

Entangled systems give
random and correlated measurement outcomes
in every measurement basis!

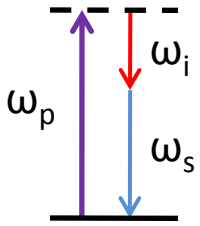
Downconversion



(a)

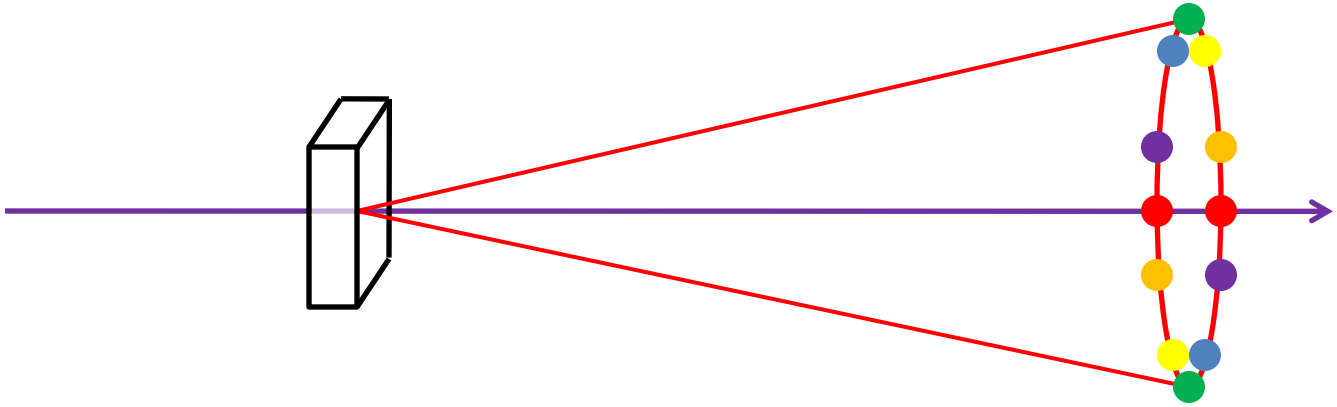


(b)



Energy
conservation

(c)

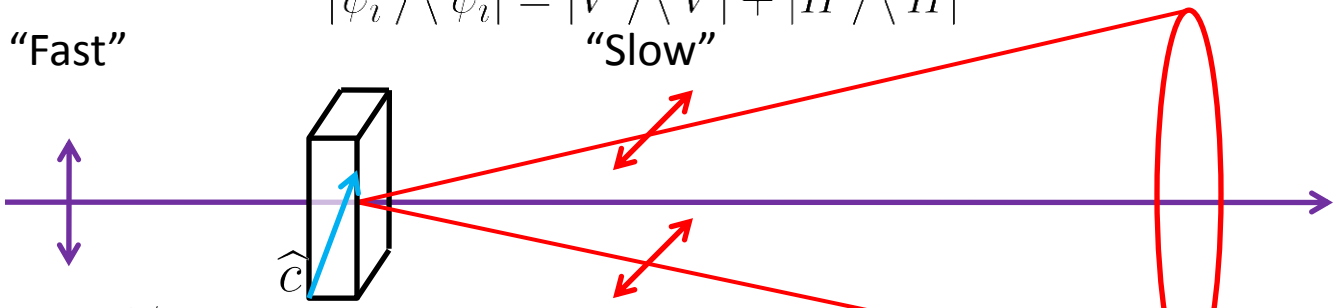


Polarization Entanglement

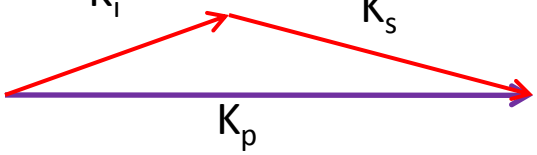
$$|\psi_i\rangle\langle\psi_i| = |V\rangle\langle V| + |H\rangle\langle H|$$

"Fast"

"Slow"

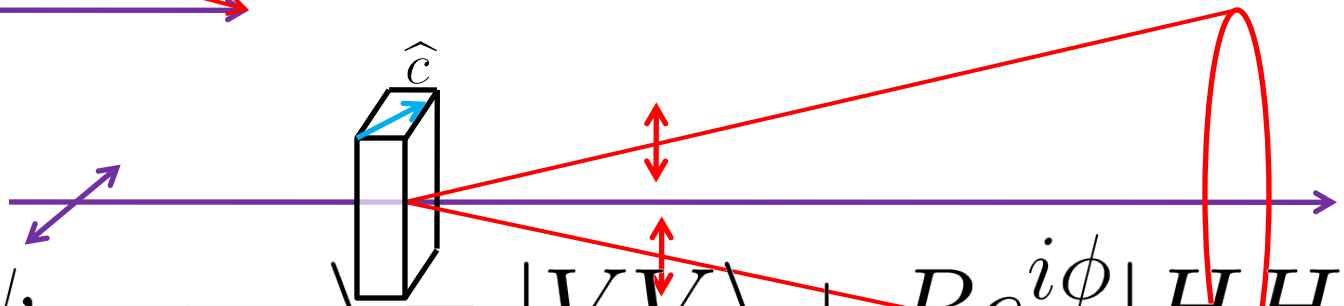


$|H\rangle + Re^{i\phi}|V\rangle$



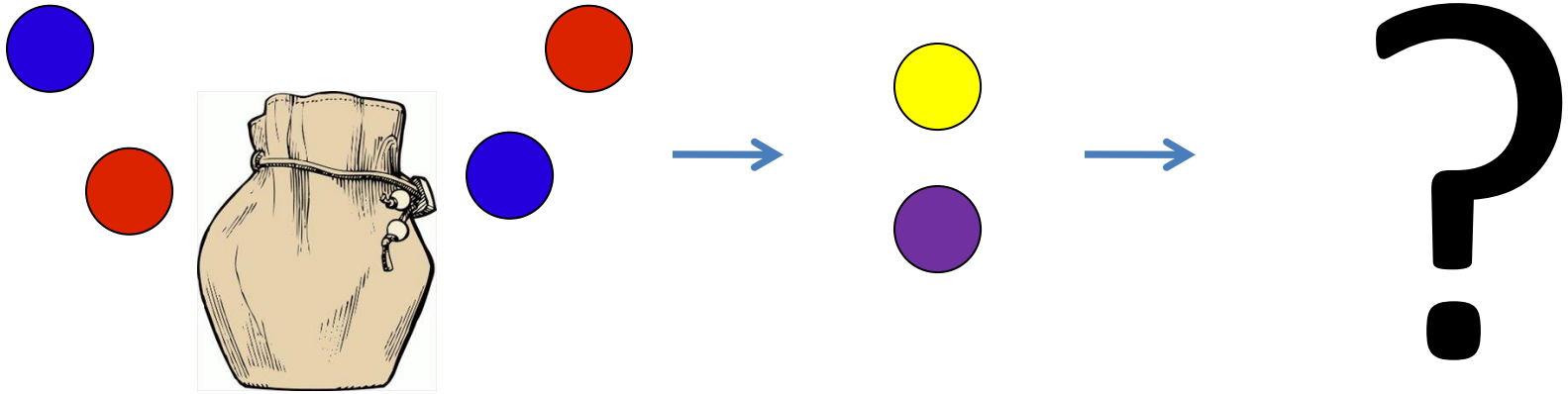
"Slow"

$$|\psi_s\rangle\langle\psi_s| = |V\rangle\langle V| + |H\rangle\langle H|$$



$$|\psi_{system}\rangle = |VV\rangle + Re^{i\phi}|HH\rangle$$

$$|HH\rangle + |VV\rangle \rightarrow \begin{matrix} |H\rangle = |D\rangle + |A\rangle \\ |V\rangle = |D\rangle - |A\rangle \end{matrix} \rightarrow |DD\rangle + |AA\rangle$$



Classical Cryptography

RSA (Rivest/Shamir/Adleman)
Public Key Cryptography

Alice: "I want to send a secure message"

Bob sends Alice a public key. The public key is tied to his private decoding key (but NOT the same)

Alice encodes her message, which Bob can decode using his private key.

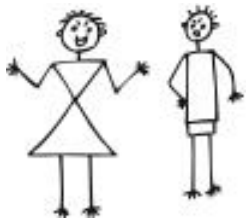
Through these public discussions, Eve tries to find out what Alice sent to Bob

Transmit message: T
Public Encryption Key: E
Private Decryption Key: D,R
$T^E = X$, where X is encrypted
where $E*D = 1 \bmod \phi(R)$,
$\phi(R)$ is Euler's Totient Function
and T,R are relatively prime
$X^D = T \bmod \phi(R)$

Finding D,R requires prime factor decomposition. Very hard computationally, but not impossible!

Classical Cryptography

One-Time Pad



Alice uses a one-time pad that she shares with Bob to encode a message.

Bob uses his identical one-time pad to decode Alice's string

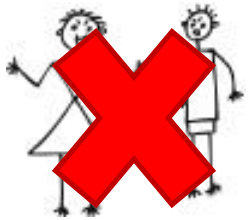
Without access to the completely random key, it is impossible for Eve to decode the string

```
Y  0 1 1 1 1 0 0 1   <-  Not random
+  1 0 0 0 1 1 1 0   <-  + Completely random
=  1 1 1 1 0 1 1 1   <-  = Completely random

   1 1 1 1 0 1 1 1   <-  Message + Secret key
-  1 0 0 0 1 1 1 0   <-  - Secret Key
   0 1 1 1 1 0 0 1  Y <-  = Message
```

~~Classical~~ Quantum Cryptography

One-Time Pad



Quantum Key Distribution

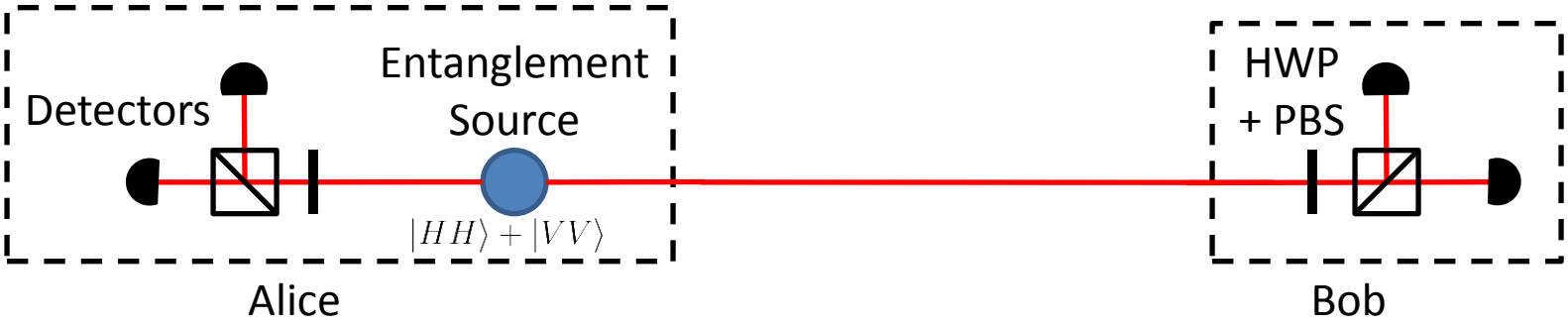
Alice uses a one-time pad that she shares with Bob to encode a message.

Bob uses his identical one-time pad to decode Alice's string

Without access to the completely random key, it is impossible for Eve to decode the string

Y 0 1 1 1 1 0 0 1	Not random
+ 1 0 0 0 1 1 1 0	+ Completely random
= 1 1 1 1 0 1 1 1	= Completely random
1 1 1 1 0 1 1 1	Message + Secret key
- 1 0 0 0 1 1 1 0	- Secret Key
0 1 1 1 1 0 0 1 Y	= Message

Quantum Key Distribution

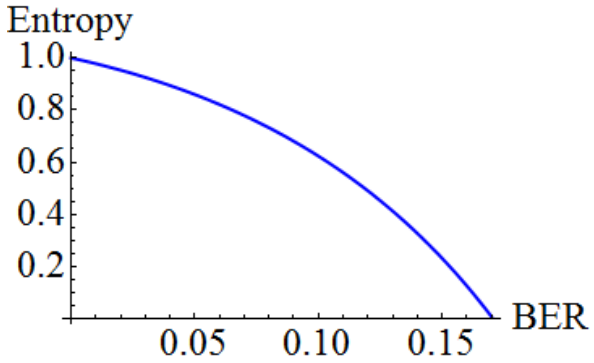


Alice's Basis Choice:	H/V	H/V
Alice's Measurements:	H	V

H/V	D/A	D/A	D/A
H	A	D	A

Bob's Basis Choice:	D/A	H/V
Bob's Measurements:	D	V

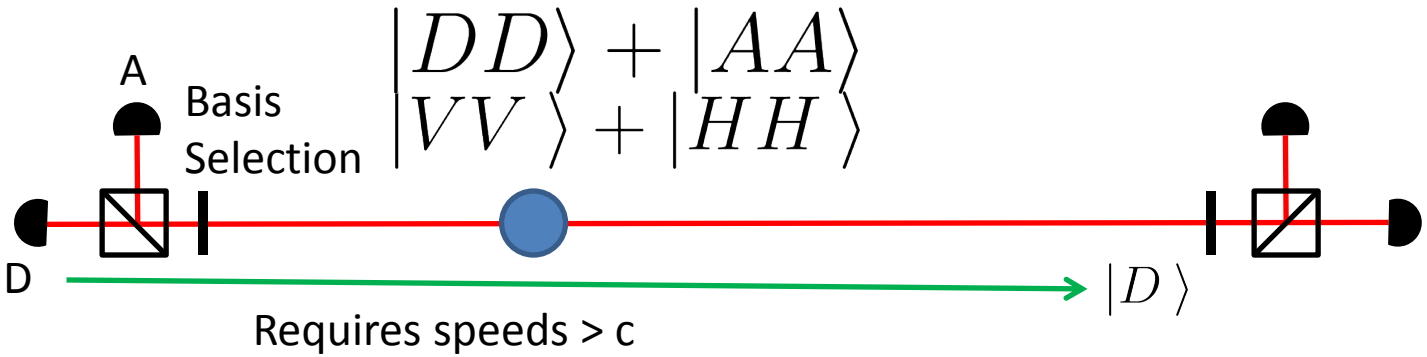
H/V	D/A	H/V	D/A
H	A	V	A



$$|DD\rangle + |AA\rangle$$
$$|VV\rangle + |HH\rangle$$

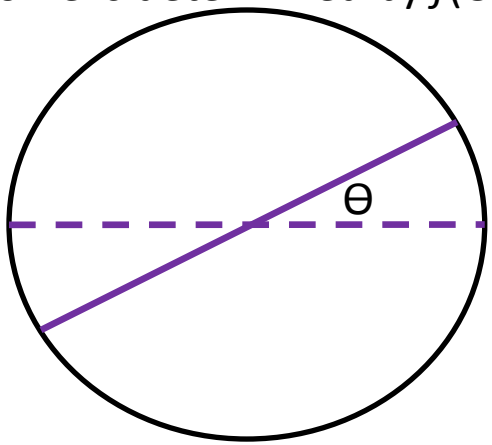
C. H. Bennett and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing", in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 175 (1984).

Hidden-Variables

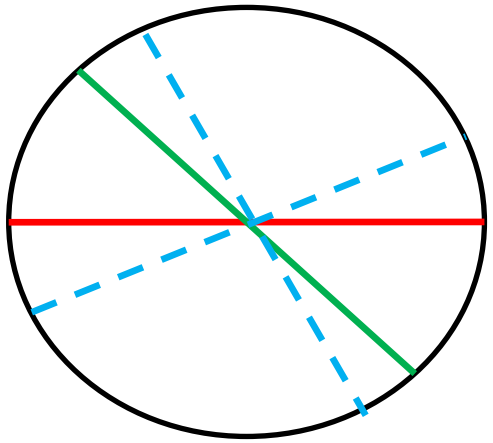


"If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity."

If measured in the Θ basis, then the outcome is determined by $f(\Theta) = \{0,1\}$



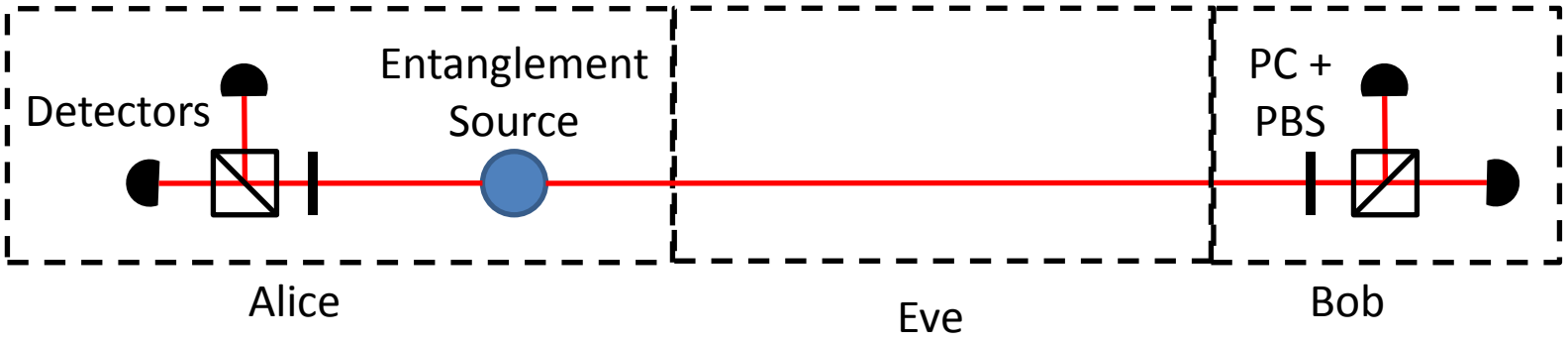
Problem:



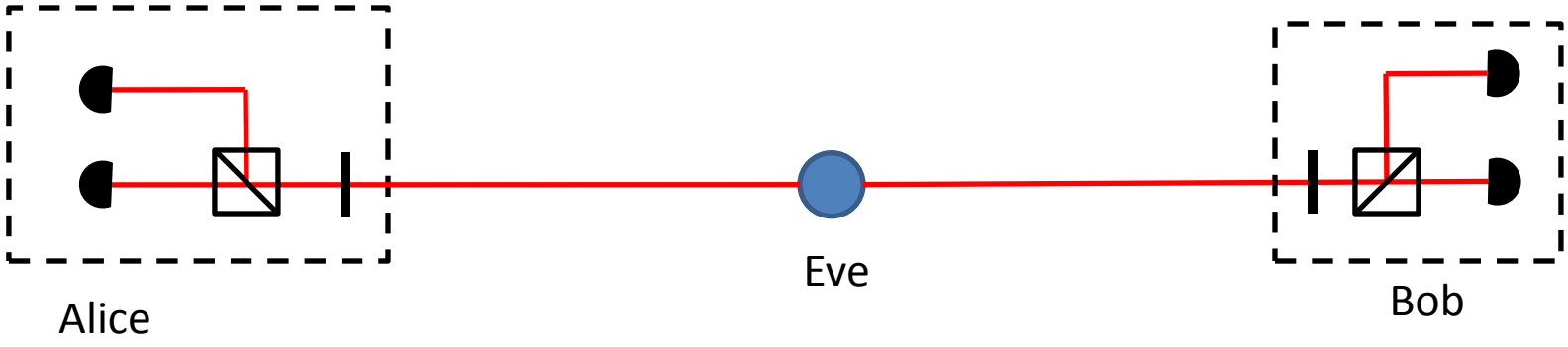
P=0.85

P=0.15

Device Independent QKD/QRNG

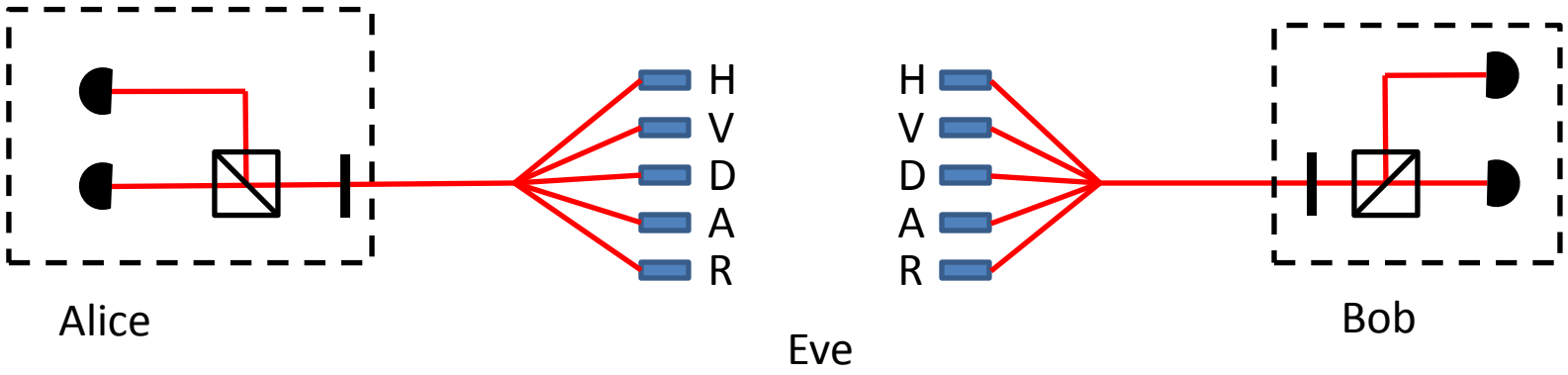


We want to remove as many assumptions as possible



Eve could pre-program the photons on where to go.
Can we detect if she does that?

Device Independent QKD/QRNG



Need to incorporate a Bell test without the detector loophole!