Unconditional Security of Quantum Key Distribution With Practical Devices

Hermen Jan Hupkes

The setting

- Alice wants to send a message to Bob.
- Channel is dangerous and vulnerable to attack.
- Message must remain secret, even if intercepted or copied.

Eve

Alice

Bob

Vernon One Time Pad

The Vernon One Time Pad is a classic example of an encryption scheme.

HI BOB
01001000 01001001 00100000 01000010 01001111 01000010 (Msg)
01110100 10111001 00000101 10101001 01011100 01110100 (Key) $\oplus$

00111100 11110001 00100101 11101011 00010011 00110110 (Encryp)

00111100 11110001 00100101 11101011 00010011 00110110 (Encryp)
01110100 10111001 00000101 10101001 01011100 01110100 (Key) $\oplus$

01001000 01001001 00100000 01000010 01001111 01000010 (Msg)
HI BOB

Vernon One Time Pad II

- If Eve does not know the key, she knows practically nothing about the message, in the following sense.

Let N be the length of the message, $m_{org} \in \{0,1\}^N \equiv \mathbb{F}_2^N$ be the original message and $m_{enc} \in \mathbb{F}_2^N$ be the encrypted message.

Write $P(m_{org} \mid m_{enc})$ for the probability that the original message is m_{org} given that the encrypted message is m_{enc}. Then

$$P(m_{org} \mid m_{enc}) = 2^{-N}.$$

- This is the best possible sense of privacy.
- Other encryption schemes exist which are more efficient in use of key.
- Sharing secret messages is thus reduced to the problem of sharing secret keys.

Key Distribution

Alice and Bob can always physically meet and exchange a long secret key.

- Impractical in current society, where millions of users are involved giving rise to billions of pairs of users.

Alice and Bob could use third person Charlie to intermediate.

- Can Charlie be trusted?

Answer: Public Key Distribution Protocols

- Alice and Bob share no initial information.
- All communication between Alice and Bob is public and can be monitored.
- At end of procedure Alice and Bob should share a secret key, which cannot be reconstructed from their public messages.

Diffie and Hellman Key Exchange

- Alice and Bob choose a (large) prime p and a generator g.
- Alice chooses randomly $1 \le k_A \le p-2$ and announces g^{k_A} mod p.
- Bob chooses randomly $1 \le k_B \le p-2$ and announces g^{k_B} mod p.
- Alice calculates key $\kappa = (g^{k_B})^{k_A}$ mod p.
- Bob calculates key $\kappa = (g^{k_A})^{k_B}$ mod p.

Theorem 1. *Breaking Diffie-Helman is equivalent to the Discrete Logarithm Problem, i.e. given a prime p, a number $2 \le g \le p-1$ and a power g^x mod p, find $x = \mathrm{Disc}\ \log g^x$.*

Example: Let $p = 7$ and $g = 3$. Then

$$\text{Disc } \log 6 = 3 \quad \text{since } 3^3 = 27 \equiv 6 \text{ mod } 7$$

Security of Diffie & Hellman

Security of Diffie and Hellman key exchange protocol is thus determined by "hardness" of the Discrete Logarithm Problem, which has been studied at great length.

Theorem 2. *The best known* ***classical*** *algorithm for solving the Discrete Logarithm Problem takes exponential time proportional to*

$$L(p) = \exp(\sqrt{\ln p} \ln \ln p).$$

This result means that making the prime p one digit longer increases the time needed to crack Diffie and Hellman by (roughly) a constant factor.

However

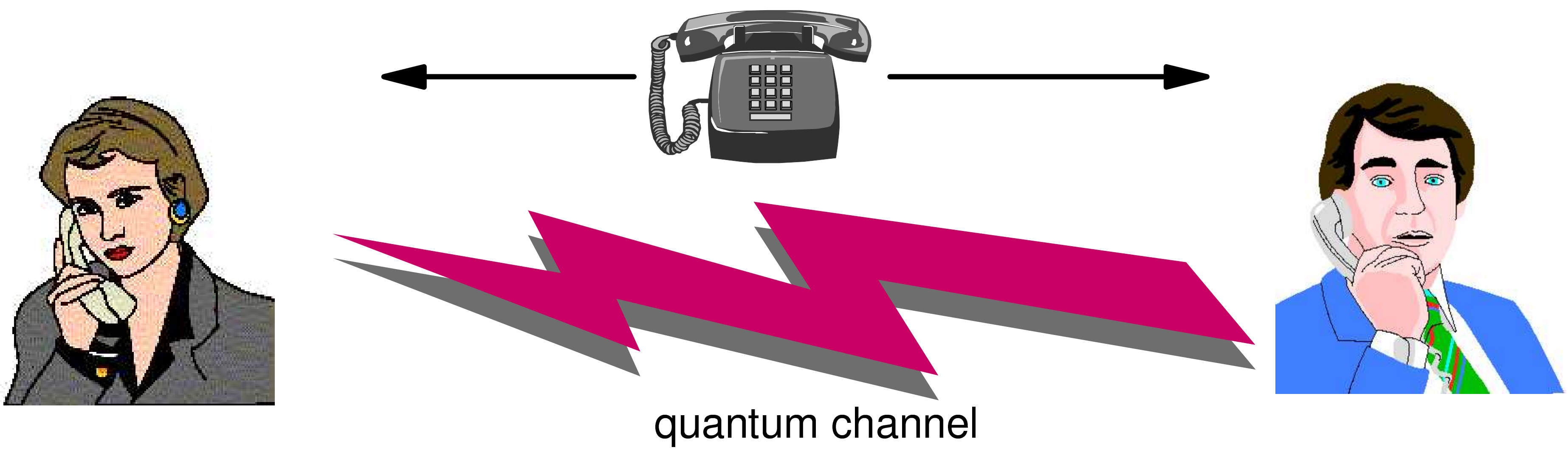
Theorem 3. *The best known* ***quantum*** *algorithm for solving DLP takes polynomial time.*

This roughly means that you have to **double** the number of digits of p every time for a fixed factor of extra running time.

Quantum Key Distribution (QKD)

Goal is to define key distribution protocol which only relies on laws of nature for its security and NOT on assumed limitations of computing power.

- Use of (vulnerable) quantum channel in addition to public classical channel.
- Alice prepares quantum states.
- Alice sends states to Bob along quantum channel.
- Bob performs measurements.
- Alice and Bob perform classical negotiation to define a key.



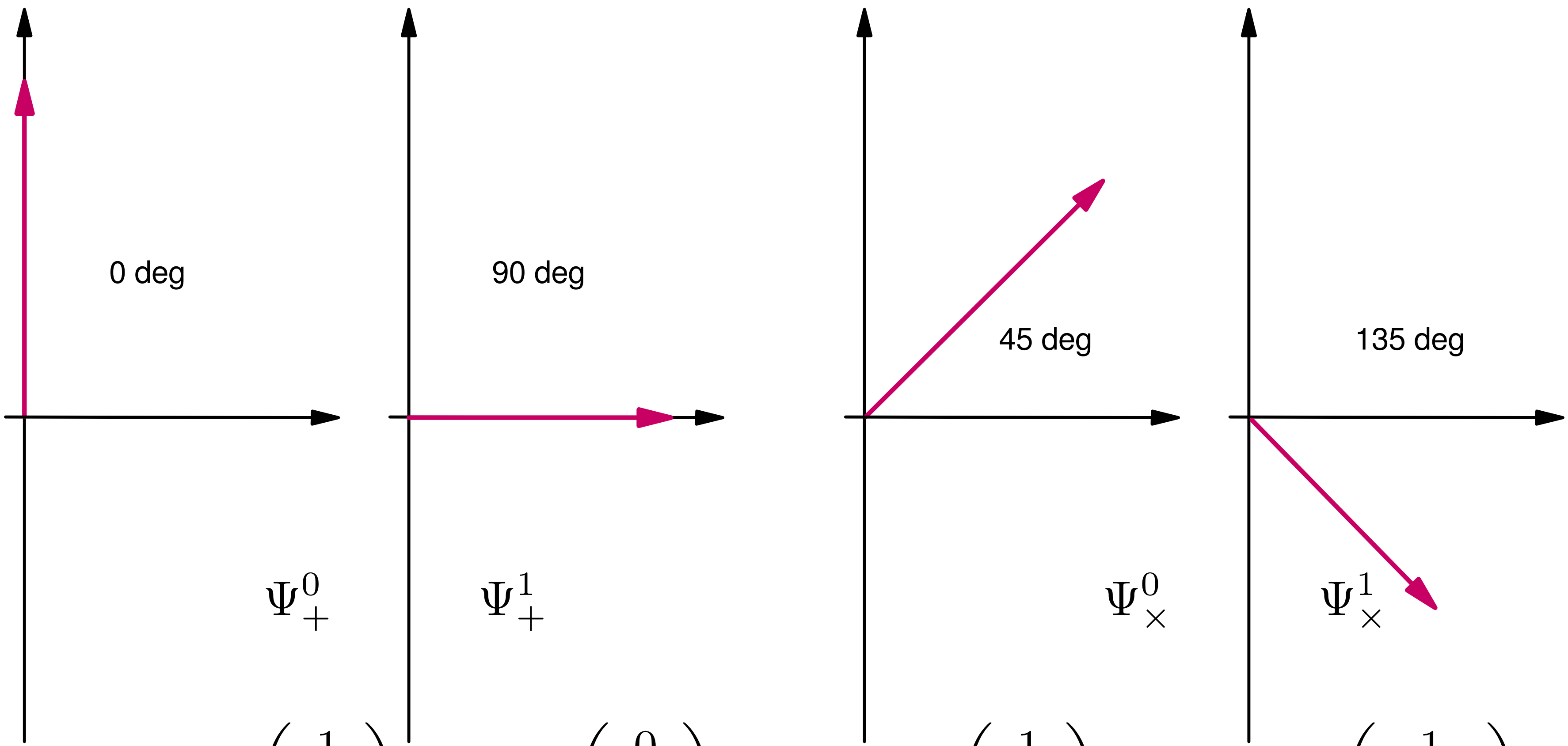
BB84 Protocol I

- Already in 1984 Brennett and Brassard proposed the BB84 QKD protocol.
- Based upon idea by Wiesner in 1960's (!). He proposed to use non-orthogonal quantum states to protect bank notes from forgery.
- No Cloning theorem. It is impossible to make a copy of an unknown quantum state.
- Today we cannot store quantum states for a long time.
- QKD only requires sending & measuring quantum states and is feasible today!
- Practical implementation over 60 km has been realized.

BB84 Protocol II - Ideal Source

Protocol requires quantum source capable of producing quantum state given basis-bit $a \in \{+, \times\}$ and key-bit $g \in \{0, 1\} \equiv \mathbb{F}_2$.

Possible implementation using **polarization encoding** on photons.



$$\psi^0_+ = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \psi^1_+ = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \psi^0_\times = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \psi^1_\times = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

BB84 Protocol III - Ideal Source

$$\psi_+^0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \psi_+^1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \psi_\times^0 = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \psi_\times^1 = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

- The states ψ_+^0 and ψ_+^1 can be perfectly distinguished from one another by measurement in $\sigma_+ = \sigma_x$ basis.
- The states $\psi_\times^0$ and $\psi_\times^1$ can be perfectly distinguished from one another by measurement in $\sigma_\times = \sigma_z$ basis.
- However,

$$\psi_\times^0 = \frac{1}{\sqrt{2}}(\psi_+^0 + \psi_+^1), \;\; \psi_\times^1 = \frac{1}{\sqrt{2}}(\psi_+^0 - \psi_+^1).$$

Measuring in wrong basis thus gives outcome 0 or 1 with equal probability.

BB84 Protocol IV - The Idea

- Choose number of photons N to exchange.
- Alice chooses N secret basis-bits $\vec{a} \in \{+, \times\}^N$.
- Bob chooses N secret basis-bits $\vec{b} \in \{+, \times\}^N$.
- Alice chooses N secret key-bits $\vec{g} \in \{0, 1\}^N = \mathbb{F}_2^N$.
- For $1 \leq i \leq N$, Alice prepares quantum state $\Psi_{\vec{a}[i]}^{\vec{g}[i]}$ and sends to Bob.
- Bob measures photon in $\vec{b}[i]$ basis and thus determines key-bits $\vec{h}[i]$.
- Alice and Bob announce all their basis-bits $\vec{a}$ and $\vec{b}$.

Note that for every position i on which Bob's and Alice's basis-bit agree, i.e. $\vec{a}[i] = \vec{b}[i]$, in absence of noise $\vec{g}[i] = \vec{h}[i]$.

Alice key-bits $\vec{g}$	**0**	**0**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**1**
Alice basis-bits $\vec{a}$	$+$	$\times$	$\times$	$\times$	$+$	$\times$	$+$	$+$	$+$	$+$	$+$	$+$	$\times$	$\times$
Bob basis-bits $\vec{b}$	$+$	$+$	$+$	$\times$	$+$	$\times$	$\times$	$\times$	$\times$	$+$	$\times$	$+$	$+$	$+$
Bob key-bits $\vec{h}$	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**

In principle, Alice and Bob can use these shared bits to define a key.

Detecting Eve

Alice and Bob need some way of checking whether Eve interfered.

$$\text{Interference} \Longrightarrow \text{Errors}.$$

- No cloning theorem guarantees that Eve cannot completely know state of photon Alice sends to Bob.

Example

- If Eve measures in σ_+ basis while Alice prepared in $\times$ basis, she will know nothing about key-bit Alice.

- Eve will also have messed up the photon that goes to Bob.

- Correlation between g and h destroyed!

The Check

- After photon exchange, Alice & Bob discard all photons for which their bases did not agree.
- Alice & Bob **randomly** choose subset R (Revealed) containing **half** of the remaining photons.
- Alice announces her key-bits $\vec{g}[R]$ for the photons in R and Bob announces his key-bits $\vec{h}[R]$.
- Alice and Bob count the number of discrepancies Δ between $\vec{g}[R]$ and $\vec{h}[R]$.
- If number of errors $\Delta > \Delta_{\mathrm{max}}$, protocol is aborted. Either Eve has been caught or too much noise.

Defining the key

If number of errors is tolerable, Alice and Bob can use remaining secret key-bits $g[\overline{R}]$ and $h[\overline{R}]$ to define a common key.

Two extra steps are necessary before this can be done.

- **Error Correction**

Due to presence of noise, must be able to compensate for a limited number of discrepancies between $g[\overline{R}]$ and $h[\overline{R}]$.

- **Privacy Amplification**

Increases further the privacy of the extracted key.

Error correction

- Goal is to protect Bob's secret key-bits from a small number of errors.
- Achieved by supplying extra information called the **syndrome**.

Example: bit-strings (x_1, x_2, x_3) of length 3. Syndrome of length two $\vec{s} = (x_1 \oplus x_2, x_1 \oplus x_3)$. One error can be corrected.

Alice	Bob
$\vec{g} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad \vec{s_A} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\vec{h} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad \vec{s_B} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad h_{corr} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$
	$\vec{h} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \vec{s_B} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad h_{corr} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$
Alice announces syndrome $\vec{s_A}$ over public channel.	$\vec{h} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \quad \vec{s_B} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad h_{corr} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$
	$\vec{h} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \vec{s_B} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad h_{corr} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$

Privacy Amplification

- Goal is to reduce information Eve has about the key.
- A private final key of length $m < n$ is constructed from Alice and Bob's n secret key-bits $\vec{g}[\overline{R}] = \vec{h}_{corr}[\overline{R}]$.

Choose a binary $m \times n$ binary matrix K. Alice and Bob define their final private key $\vec{\kappa}$ by

$$\vec{\kappa_A} = K\vec{g}, \quad \vec{\kappa_B} = K\vec{h}_{corr}.$$

If error correction was succesfull, we have $\vec{\kappa_A} = \vec{\kappa_B}$.

$$m = 2, \;\; n = 4, \;\; K = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

$$\vec{g} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \Longrightarrow \vec{\kappa_A} = K\vec{g} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Even if Eve happens to know one bit of $\vec{g}$, this helps her nothing!

BB84 Summary

- Alice & Bob choose number of photons to exchange N.
- Alice & Bob choose random secret strings $\vec{a}, \vec{b} \in \{+, \times\}^N$ and $\vec{g} \in \mathbb{F}_2^N$.
- Alice sends photons in state $\psi_{a[i]}^{g[i]}$ and Bob measures, determining $\vec{h} \in \mathbb{F}_2^N$.
- Alice & Bob discard useless photons, choose subset R and perform eavesdropping test. If error rate is too high, protocol is aborted.
- Alice & Bob agree on error-correcting code.
- Alice announces syndrome $\vec{s}$ and Bob applies error correction.
- Alice & Bob choose privacy amplification matrix K and calculate the final key $\kappa = K\vec{g} \approx K\vec{h}_{corr}$.

Privacy I

Need exact and suitable notion of privacy.

- Eve can never infer Alice and Bob's key with more than $X\%$ confidence.

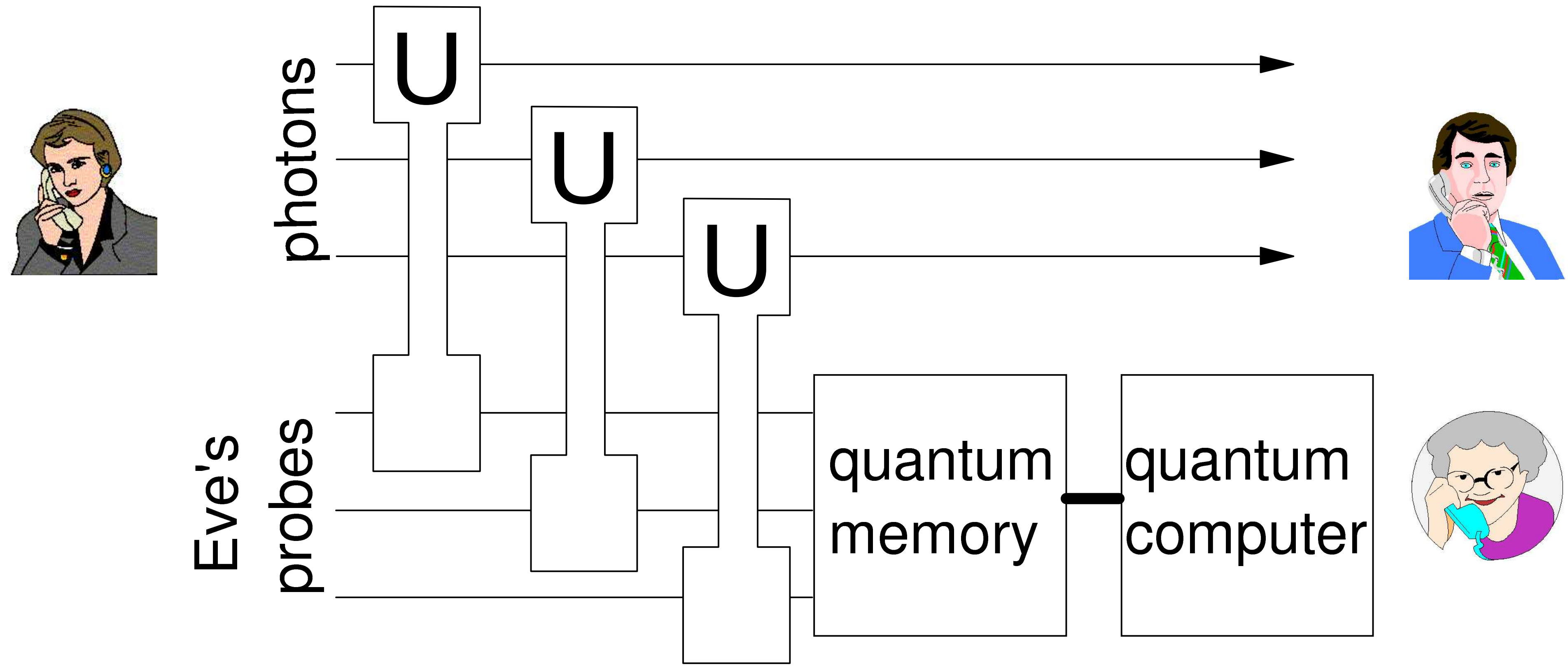
Too strong. Consider an attack in which Eve always measures in σ_+ basis and resends a photon to Bob polarized according to the measurement result. If $\vec{a} = (+, +, \ldots, +)$, Eve is lucky and gets to know key.

Eve can always randomly guess the key κ. She will then have probability 2^{-m} of success, where m is the length of the final key κ.

Need probabilistic notion of privacy, saying that Eve can not do much better than simply guess the key.

Thus we want $P_{succ} \approx 2^{-m}$.

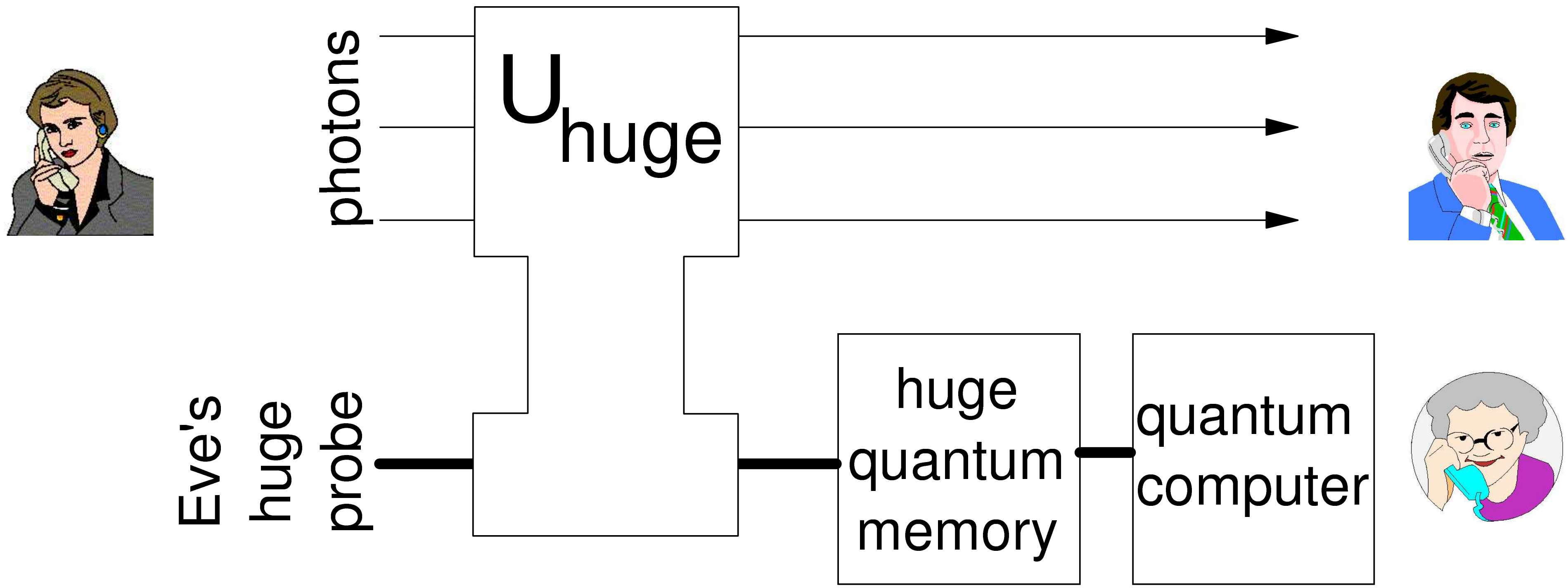
Eve's attack



Collective attack.

- Eve attaches probe to each photon individually.
- Eve stores probe during classical communication between Alice & Bob.
- Eve allowed to perform combined measurement on the probes afterwards.

Eve's strongest attack

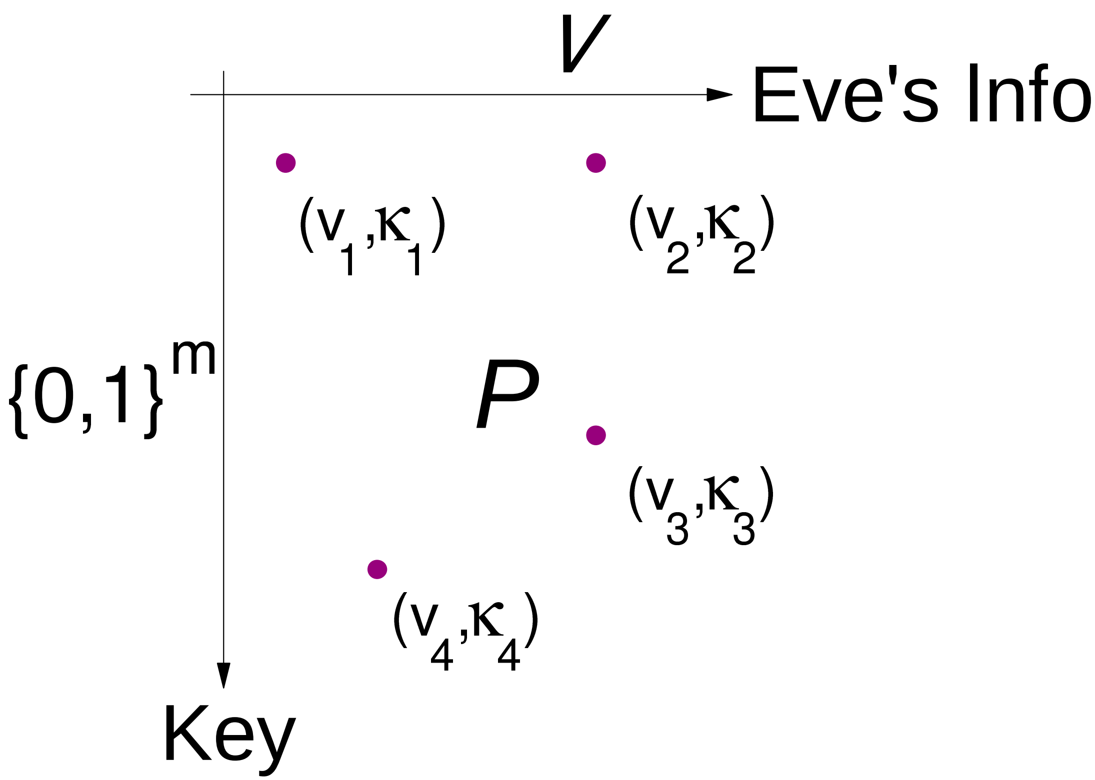


Coherent attack.

- Most general option available to Eve.
- Eve can perform any measurement she wants on photons, probes and external systems.
- Includes random attacks!

Privacy II

After eavesdropping, Eve has obtained some information $v \in \mathcal{V}$ and the final key $\vec{\kappa}$ is determined by Alice.

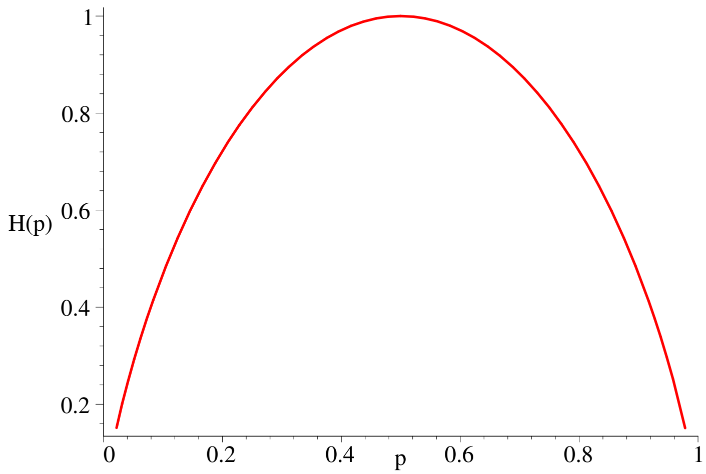


Eve's tactic defines a probability distribution P on the set $\mathbb{F}_2^m \times \mathcal{V}$.

$P(\vec{\kappa}, v)$ denotes the probability that the final key is $\vec{\kappa}$ while the information gathered by Eve is v.

We want independence of $\vec{\kappa}$ and v, i.e. $P(\vec{\kappa}, v) \approx P(\vec{\kappa})P(v) = 2^{-m}P(v)$.

Entropy



The two-bin entropy

$$H^{(2)}(p) = -(p \log_2 p + (1-p)\log_2(1-p)).$$

Maximal value for $p = \frac{1}{2}$ i.e. equal distribution over the bins.
Entropy measures "flatness" of distribution!

Measure for privacy: Conditional Shannon Entropy

$$H = \sum_{v \in \mathcal{V}} P(v) \sum_{\kappa \in \mathbb{F}_2^m} \Big(- P(\kappa \mid v) \log_2 P(\kappa \mid v) \Big) = \sum_{v \in \mathcal{V}} P(v) H(v).$$

- Key κ and Eve's view v independent $\Longrightarrow P(\kappa|v) = 2^{-m} \Longrightarrow H = m$.
- For every v, we want flat $P(\kappa \mid v)$, i.e. large $H(v)$.
- Conditional Entropy H can be seen as weighted average over these "flatnesses".
- Want $H \approx m$, the maximal value.

Privacy III

Definition 1. The BB84 protocol is **private** if there exist positive C, λ, $N_{\min}$ such that, for **any** eavesdropping strategy employed by Eve

$$m - H \leq Ce^{-\lambda N} \text{ for all } N \geq N_{\min},$$

for fixed ratio m/N. $\square$

- Recall m is length of final private key and N is number of exchanged photons.
- The ratio m/N is called the **key-generation rate**.
- Increasing N with fixed key-generation rate thus exponentially increases the level of privacy.

History

1984 Brennett and Brassard propose BB84 scheme.

<1998 Many particular types of attacks analyzed (e.g. collective attack). No general privacy result.

1998 Mayers gives first proof of privacy against arbitrary attack by Eve. However, he assumes that the quantum source is **perfect**. The detector is left **uncharacterized**.

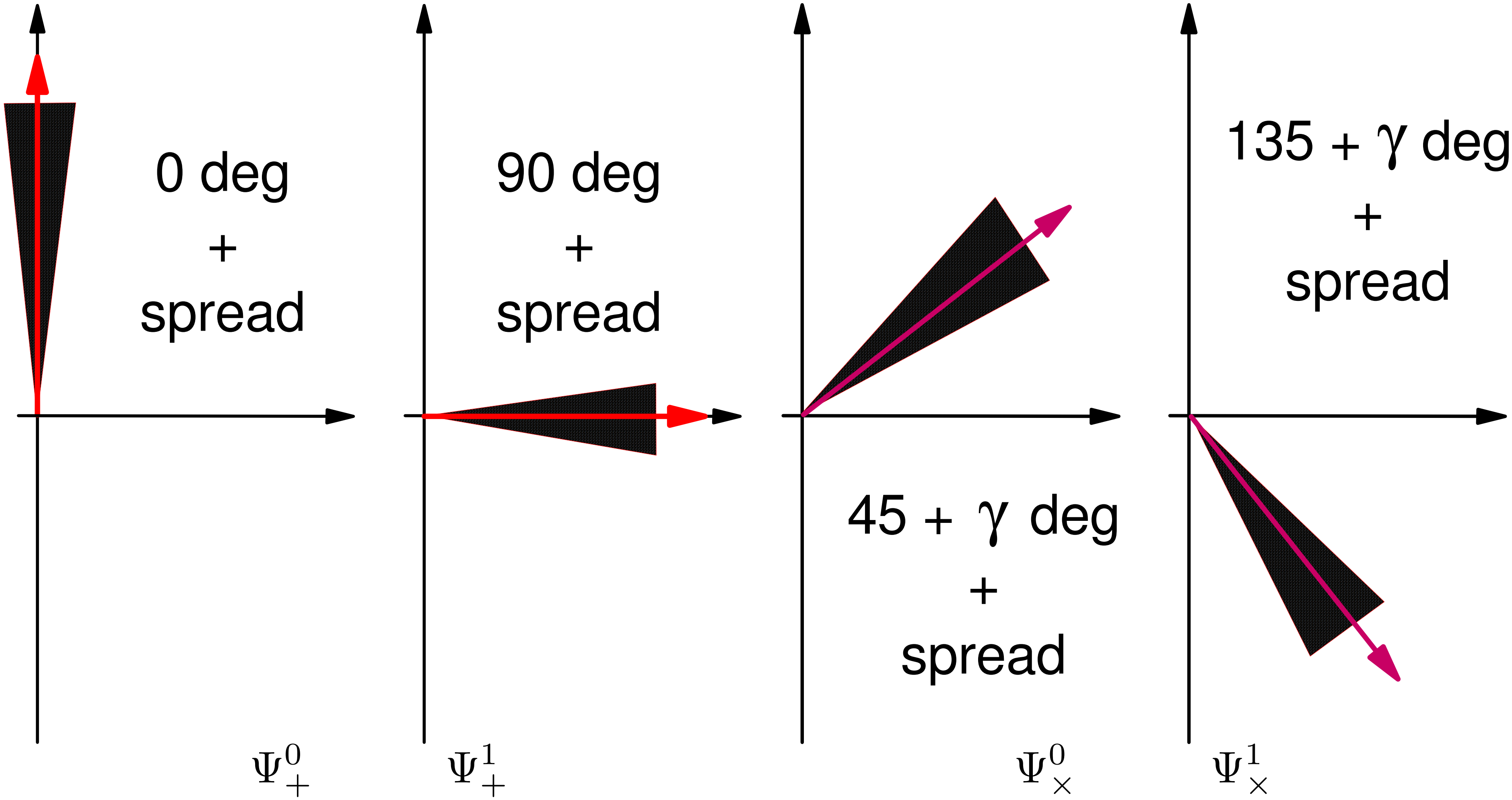
Beautiful separation between privacy and practicality (how often does the verification test pass).

<2002 More privacy proofs (Shor, Preskill) for specific source / detector models.

2002 Koashi and Preskill prove privacy for perfect detector.

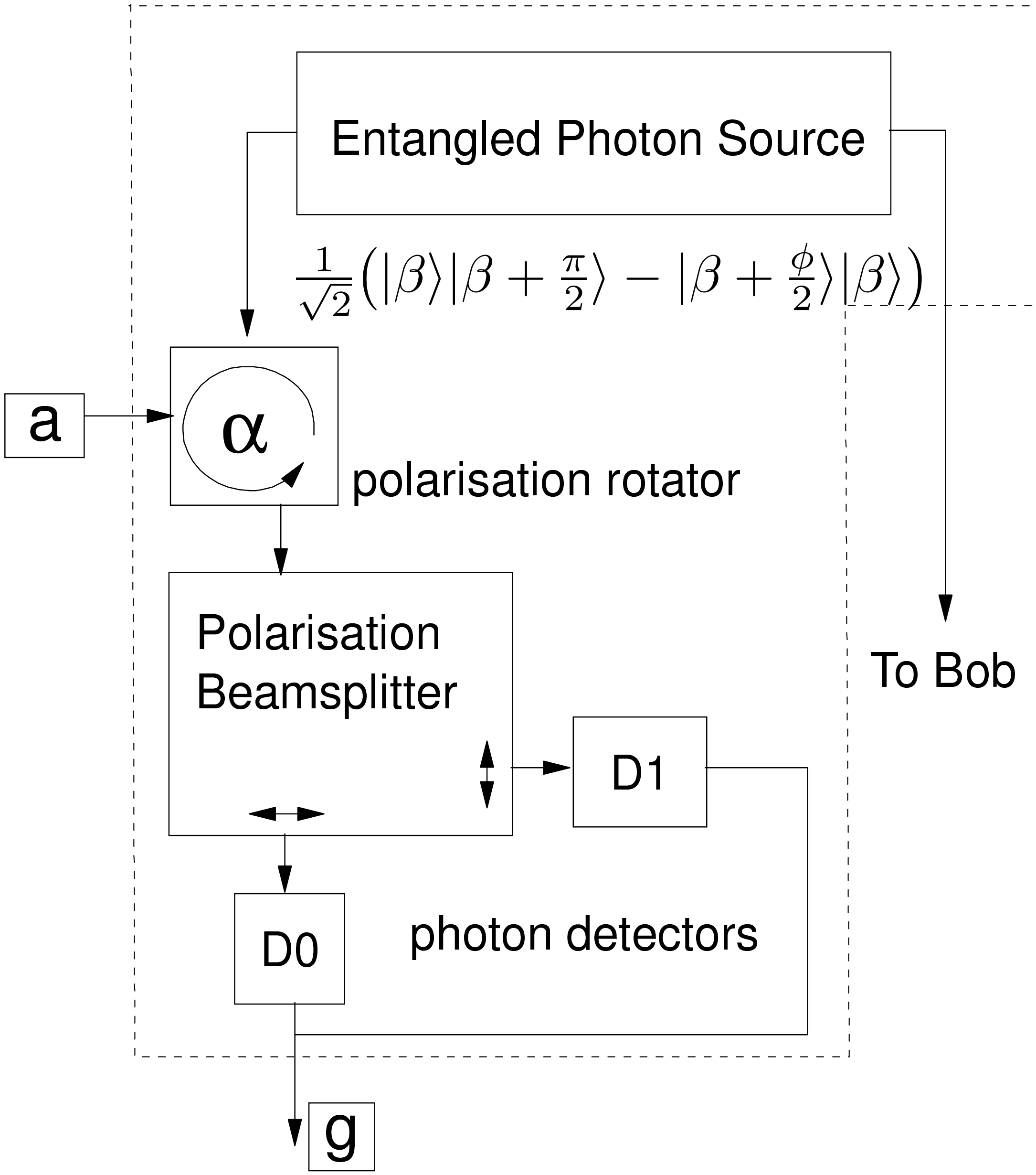
2004 Hupkes: Extension of Mayers' result to include class of non-perfect sources. Detector is left uncharacterized.

Quasi-Perfect Sources - Example



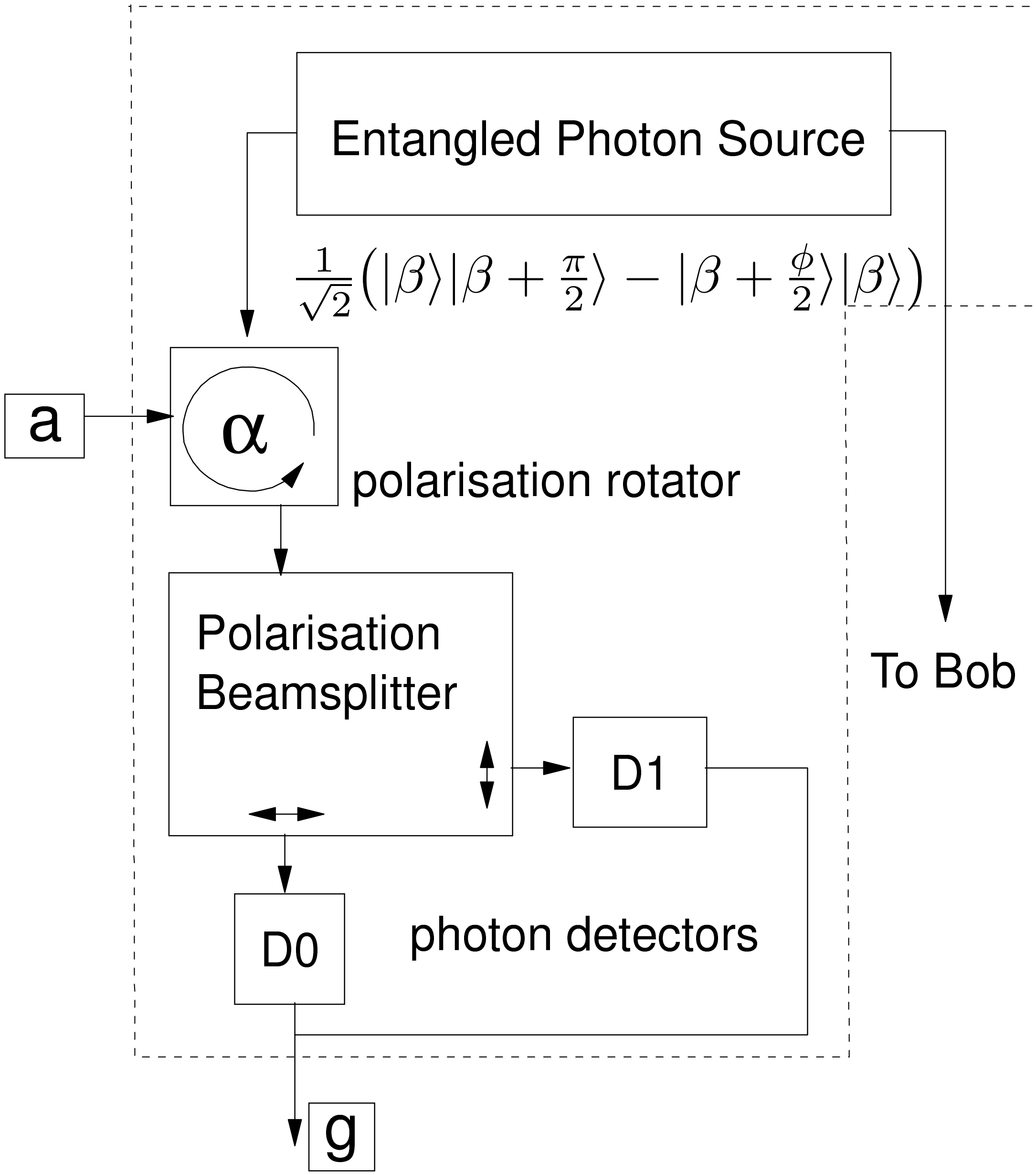
- No longer require **exact** polarization.
- No longer require **exact** 45 degree difference between bases.
- However, both two states corr. to same basis-bit must have **same** spread.

Possible Implementation



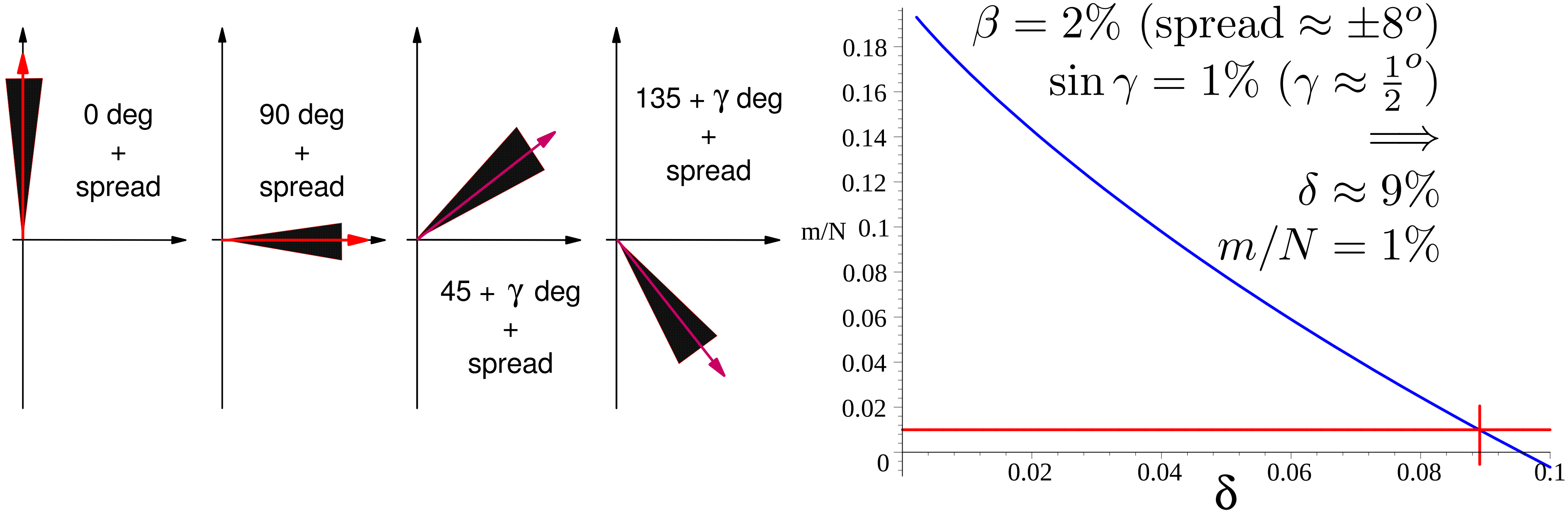
- Entangled photon pair with orthogonal polarizations produced by e.g. parametric downconversion.
- Alice sets $\alpha = a\frac{\pi}{4}$.
- Alice performs polarization measurement on her photon to determine g.
- Other photon sent to Bob.
- Bob's photon polarized at $|\alpha\rangle$ or $|\alpha+\frac{\pi}{2}\rangle$, depending on outcome measurement Alice.

Why Quasi-Perfect Source



- In practice, perfect polarization encoding is impossible.
- Need to deal with uncertainties in equipment (for example, rotation angle α). This is covered by introduction of spreads around ideal value.
- Need to deal with possibility that Eve might have tampered with source. She might have chosen to set $\alpha = \frac{\pi}{4} + \gamma$ if $a = 1$.

Main Result



Theorem 4. *For small offset angles γ and small spreads in the distributions, the BB84 protocol is private under suitable operating conditions. One can generate keys with the rate*

$$m/N = \frac{1}{4}\Big(1 - H^{(2)}(\delta) - H^{(2)}(\delta + \beta + \sin\gamma)\Big),$$

where δ is the threshold for the validation test and $\beta =< \sin^2(\text{spread}) >$ measures the distribution spread.

Remaining Issues

- How can one test if a source is quasi-perfect?

-Mayers et al introduced way to check if source is an ideal BB84 source. However, they need an **exact** measurement. Can possibly be usefully generalized to quasi-perfect sources.

- What about multi-photon emissions? In practice, single photon sources very hard to make.

-Mayers et al. : Small number of multi-photon pulses does not destroy privacy for perfect polarization encoding. Can hopefully easily be adapted to quasi-perfect sources.

The End