Title: Quantum key distribution protocols with and without rotational

Date: Nov 29, 2006 04:00 PM

URL: http://pirsa.org/06110040

Abstract: We explore the role of rotational symmetry of quantum key distribution (QKD) protocols in their security. Specifically, in the first part of the talk, we consider a generalized QKD protocol with discrete rotational symmetry. Note that, before our work, each QKD protocol seems to have a different security proof. Given that the techniques of those proofs are similar, it will be interesting to have a unified proof for QKD protocols with symmetry (e.g., the BB84 protocol and the SARG04 protocol). This is exactly what we achieve in our work. We show that rotational symmetry plays an important role in the unified security proof of QKD protocols with symmetry, leading to simple and structural security relations. In the second part, we consider a QKD protocol that does not possess rotational symmetry and analyze its security. Interestingly, even without any rotational symmetry, this protocol can still be proven secure. However, the security relation is not as simple as those in the first part, due to the lack of symmetry. Therefore, although rotational symmetry is not required in a QKD protocol to ensure its security, rotational symmetry does provide significant simplification in the security analysis, leading to simple security relations.

Outline

- Introduction to QKD protocols
- Motivation for studying rotational symmetry in QKD protocols
- Protocol 1: Generalized QKD protocol
- Protocol 2: Three-state protocol
- Secret key generation rate
  - Single-photon source
  - Coherent light source
- Conclusion

Outline

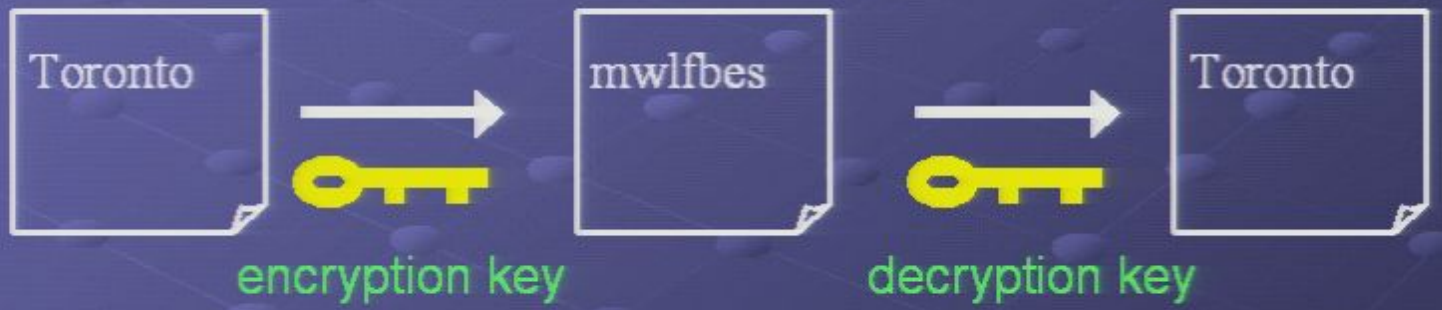
- Introduction to QKD protocols
- Motivation for studying rotational symmetry in QKD protocols
- Protocol 1: Generalized QKD protocol
- Protocol 2: Three-state protocol
- Secret key generation rate
  - Single-photon source
  - Coherent light source
- Conclusion

What is wrong with conventional cryptography?

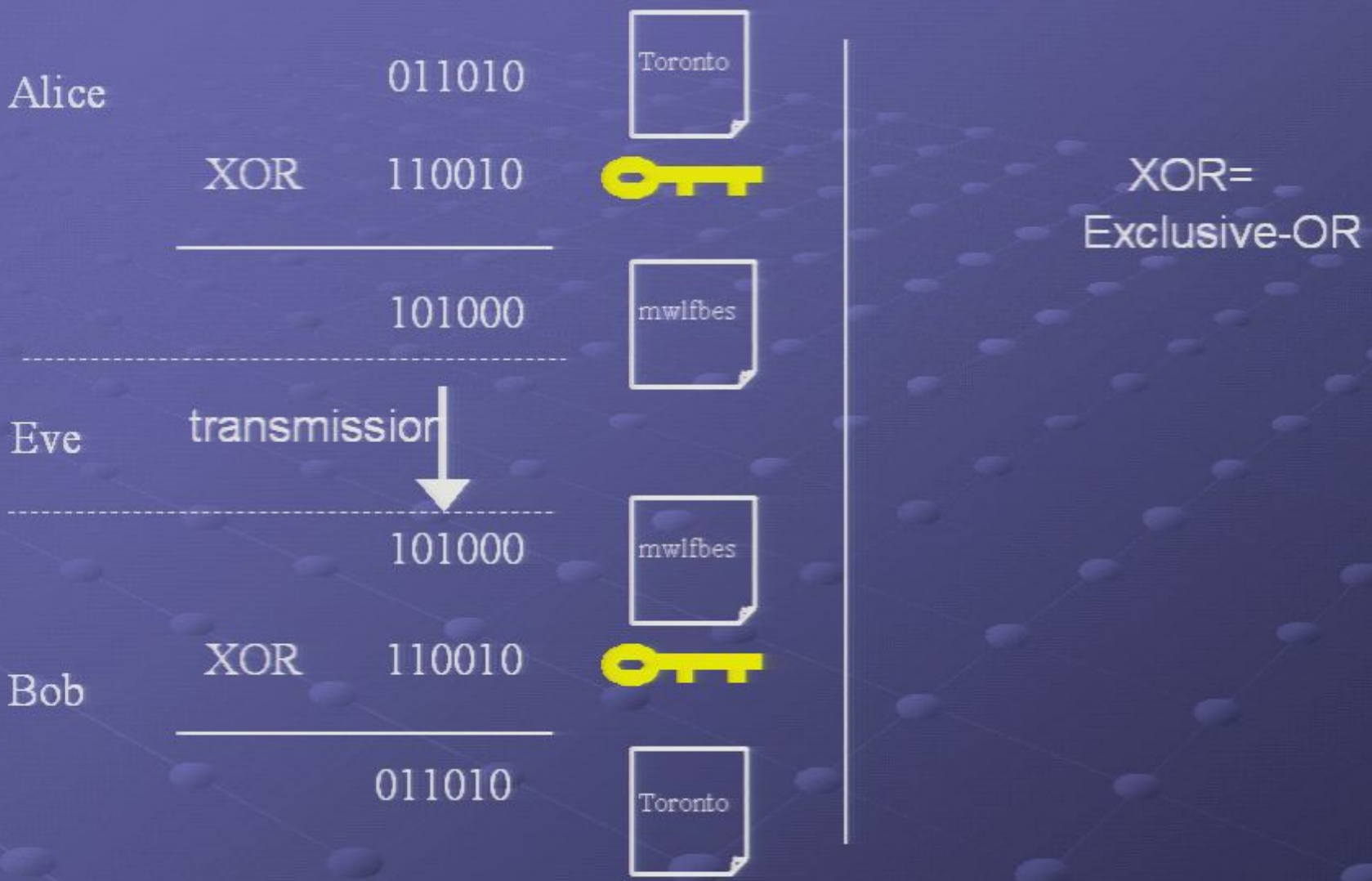
1. Unanticipated Advances in Hardware and Algorithms.
2. Quantum Code-breaking:
   (Shor 1994) quantum computers can efficiently factor large numbers, thus breaking RSA, the best-known public key cryptography.

``If a quantum computer is ever built, much of conventional cryptography will fall apart!'' (Brassard)

Key Distribution Problem

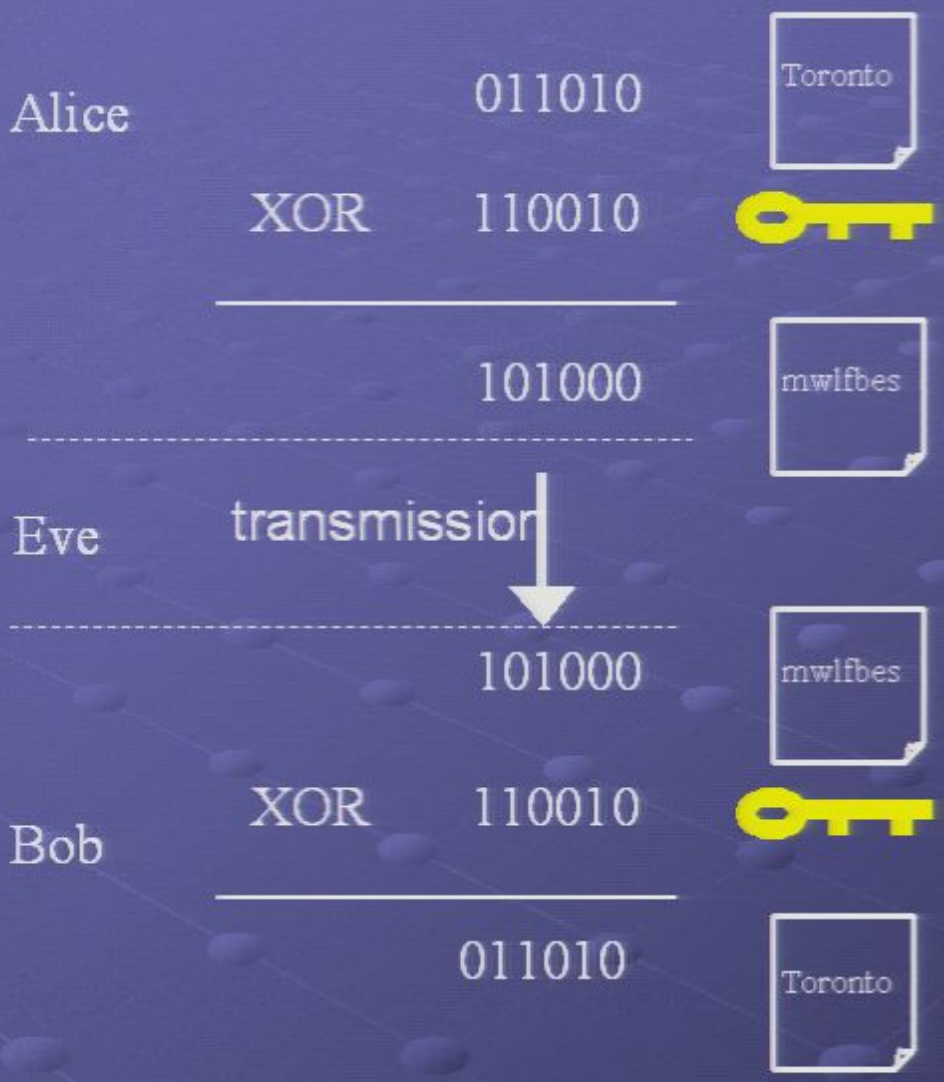


One-time pad



XOR=
Exclusive-OR

One-time pad



XOR=
Exclusive-OR

If Alice and Bob share a common long random string of secret, then One-time-pad method is perfectly secure. (Shannon 1949)

QUESTION: How to transfer the key?

Quantum key distribution (QKD)

- Absolute security based on fundamental laws of quantum mechanics, rather than computational assumptions.
- Allow two persons who share a small amount of authentication information to communicate in absolute security in the presence of an eavesdropper.
- Any eavesdropping attack will essentially always be caught.

Alice

Bob

Quantum key distribution (QKD)

- Absolute security based on fundamental laws of quantum mechanics, rather than computational assumptions.
- Allow two persons who share a small amount of authentication information to communicate in absolute security in the presence of an eavesdropper.
- Any eavesdropping attack will essentially always be caught.

Intrusion alert!

Eve

Intrusion alert!

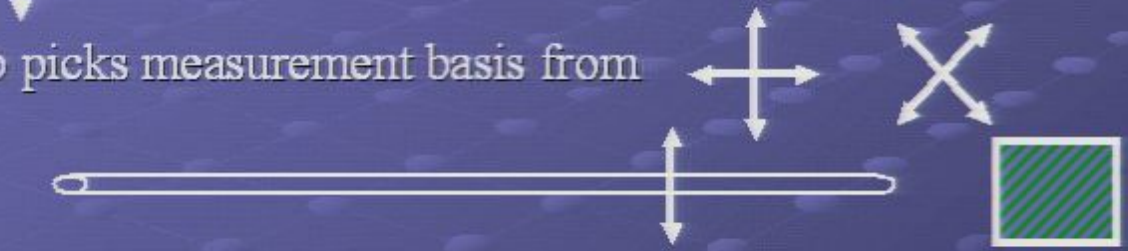
Alice

Bob

Procedure of standard BB84 QKD scheme (Sketch)

Step 1: Alice picks photon polarization from

Step 2: Bob picks measurement basis from



Step 3: Bob records his basis and measurement outcome.

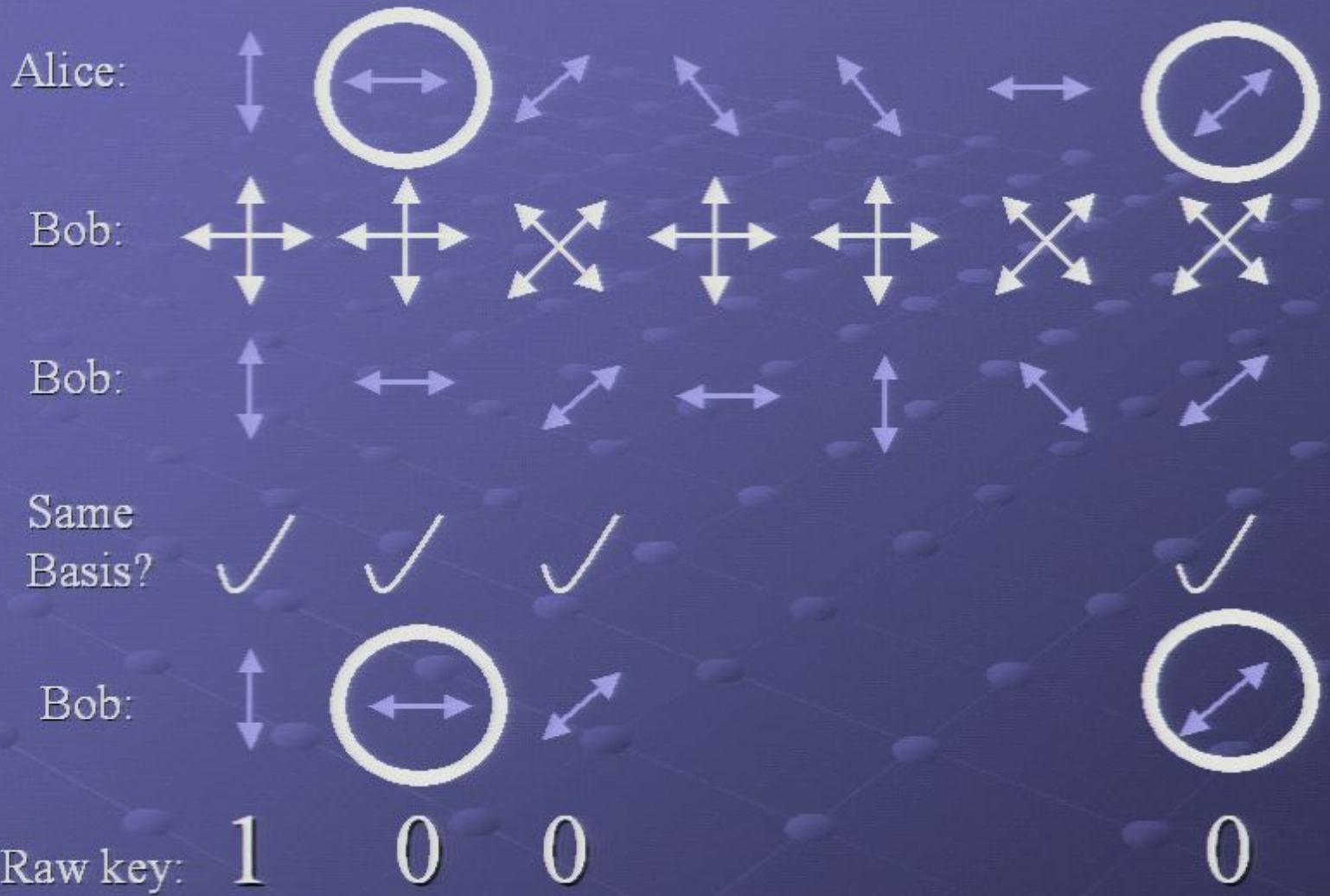
basis outcome

Step 4: Alice and Bob announce their bases publicly. They keep only the polarization data when they have used the same basis.

Step 5: Test for tampering by random sampling and computing quantum bit error rate. If error rate is OK, apply error correction and "privacy amplification".

Schedule of BB84 scheme

Test for tampering



Broadcast and Compare a subset of signals.
Deduce error rate of transmission

Proof of unconditional security of BB84

1. Mayers, J. of ACM, vol. 48, no. 3, pp. 351-406; preliminary version Crypto'96.
2. Lo and Chau, Science 283, 2050 (1999).
3. Shor and Preskill, Phys. Rev. Lett. 85, 441 (2000).

In summary, BB84 is proven to be secure

Outline

- Introduction to QKD protocols
- Motivation for studying rotational symmetry in QKD protocols
- Protocol 1: Generalized QKD protocol
- Protocol 2: Three-state protocol
- Secret key generation rate
  - Single-photon source
  - Coherent light source
- Conclusion

Rotational symmetry

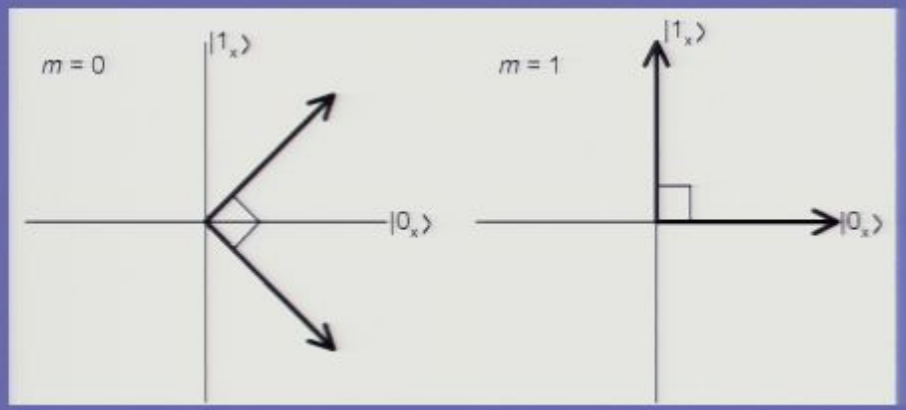
- Many well-known QKD protocols possess rotational symmetry (e.g. BB84, SARG04)

Rotational symmetry

- Many well-known QKD protocols possess rotational symmetry (e.g. BB84, SARG04)

BB84

[Bennett and Brassard (1984)]

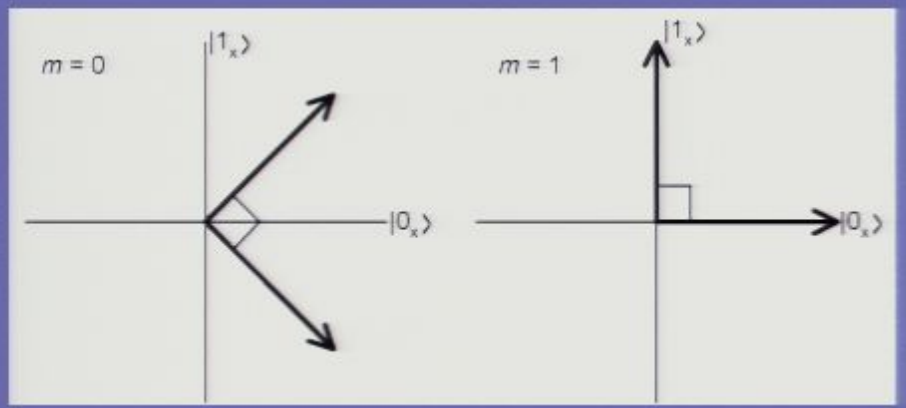


Rotational symmetry

- Many well-known QKD protocols possess rotational symmetry (e.g. BB84, SARG04)

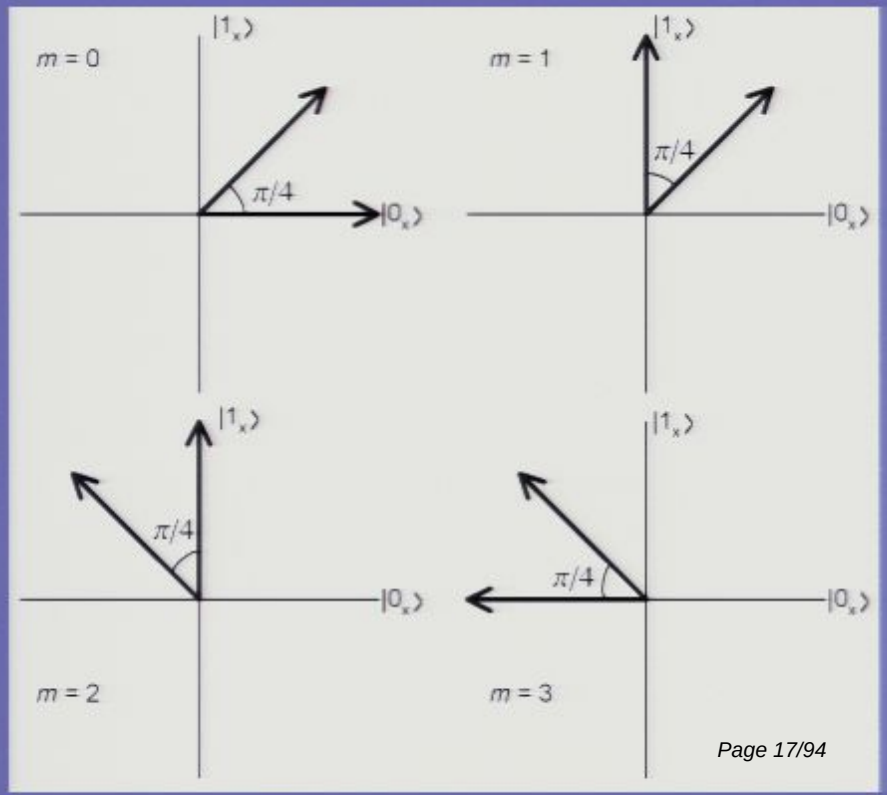
BB84

[Bennett and Brassard (1984)]



SARG04

[Scarani, Acin, Ribordy, Gisin, (2004)]



Motivation for studying rotational symmetry

- Many security proofs rely on rotational symmetry
- $\Rightarrow$ Intimate relationship between rotational symmetry and the security of QKD protocols

Questions:

Motivation for studying rotational symmetry

- Many security proofs rely on rotational symmetry
- $\Rightarrow$ Intimate relationship between rotational symmetry and the security of QKD protocols

Questions:

1. Can we prove security of a ***generalized*** QKD protocol with rotational symmetry?

Motivation for studying rotational symmetry

- Many security proofs rely on rotational symmetry
- $\Rightarrow$ Intimate relationship between rotational symmetry and the security of QKD protocols

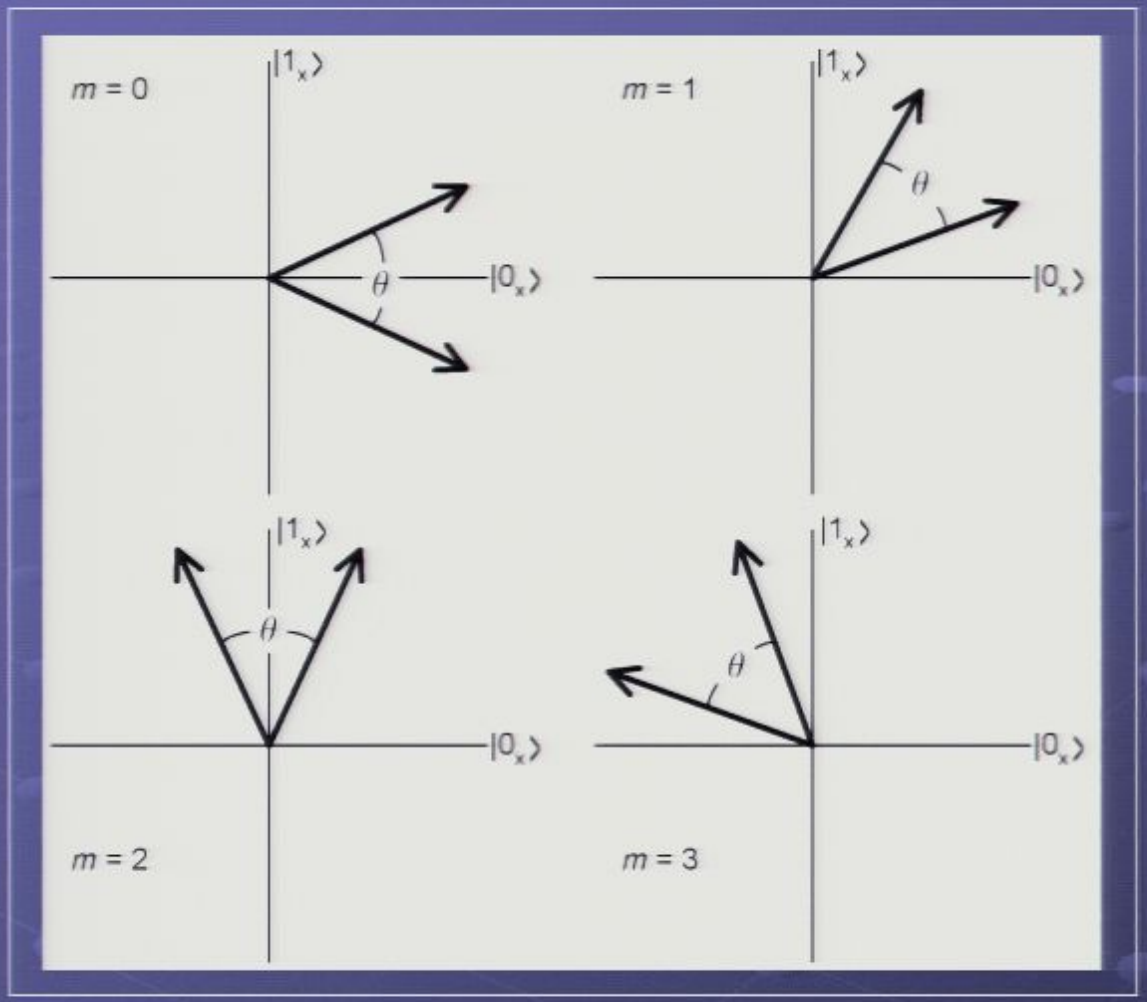
Questions:

1. Can we prove security of a ***generalized*** QKD protocol with rotational symmetry?
2. Can we prove security of a QKD protocol ***without*** rotational symmetry?

Outline

- Introduction to QKD protocols
- Motivation for studying rotational symmetry in QKD protocols
- Protocol 1: Generalized QKD protocol
- Protocol 2: Three-state protocol
- Secret key generation rate
  - Single-photon source
  - Coherent light source
- Conclusion

Protocol 1: Generalized QKD Protocol



- Arbitrary number of bases (M)
- Arbitrary angle between basis states (θ)
- All the bases are even spaced within an angle of π

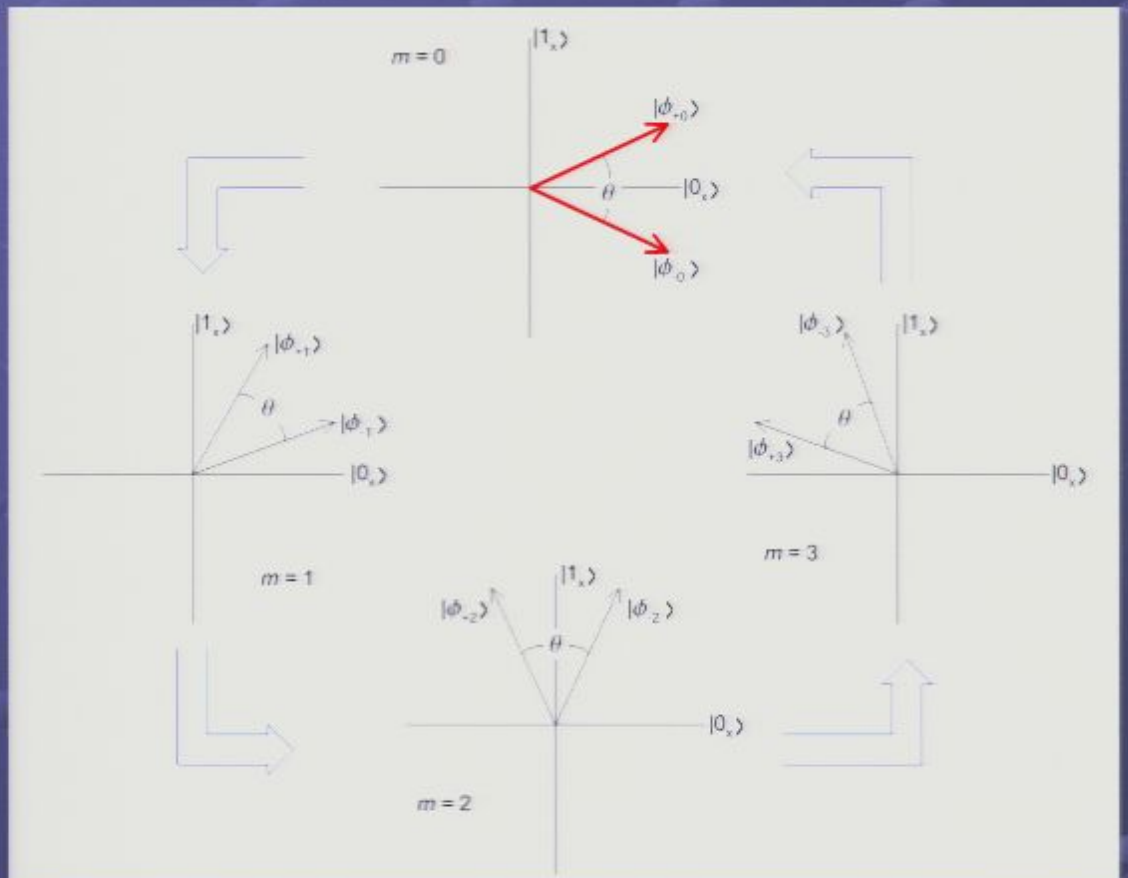
Property of Generalized QKD Protocol

- The next basis is generated by rotating the current basis by π/M.

Property of Generalized QKD Protocol

Rotational symmetry

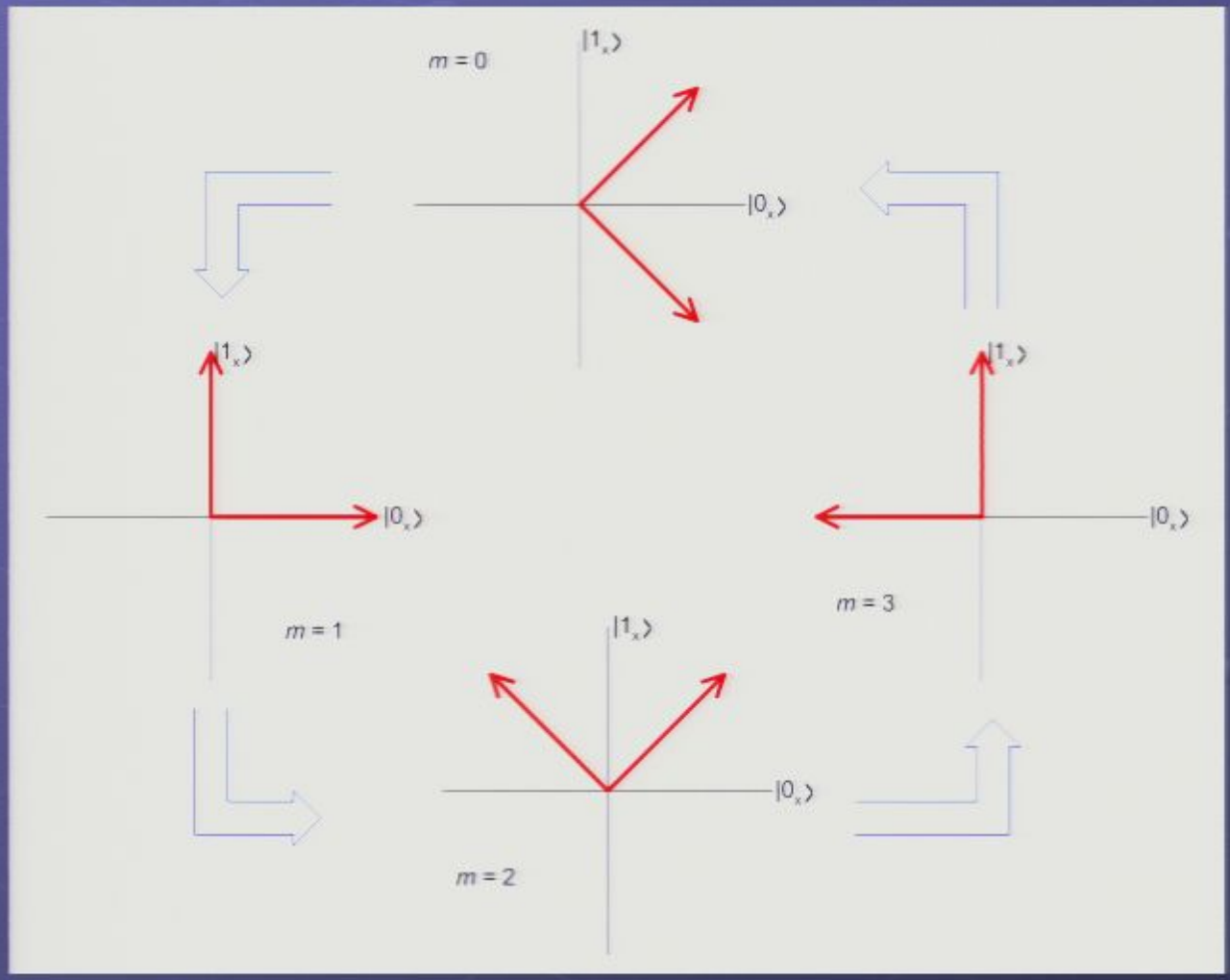
- The next basis is generated by rotating the current basis by π/M.



Protocol 1: Generalized QKD Protocol

- The generalized QKD protocol includes many well-known protocols as specific cases
- E.g. BB84 (a symmetrized version) with M=4 and $\theta=\pi/2$
- E.g. SARG04 with M=4 and $\theta=\pi/4$

BB84 (a symmetrized version) with M=4 and $\theta=\pi/2$

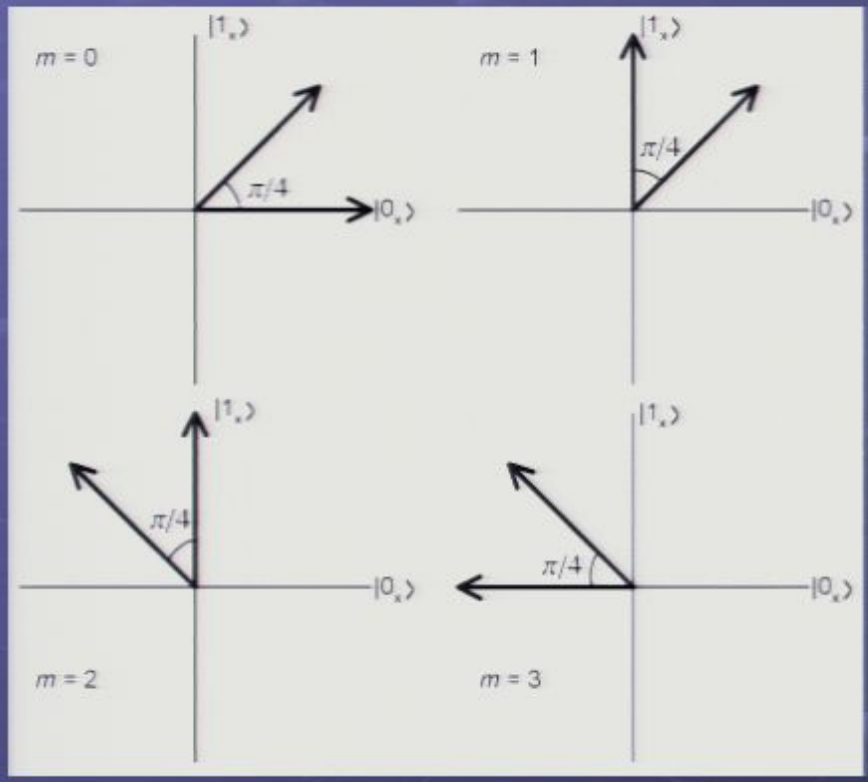


= normal BB84 with two bases

SARG04

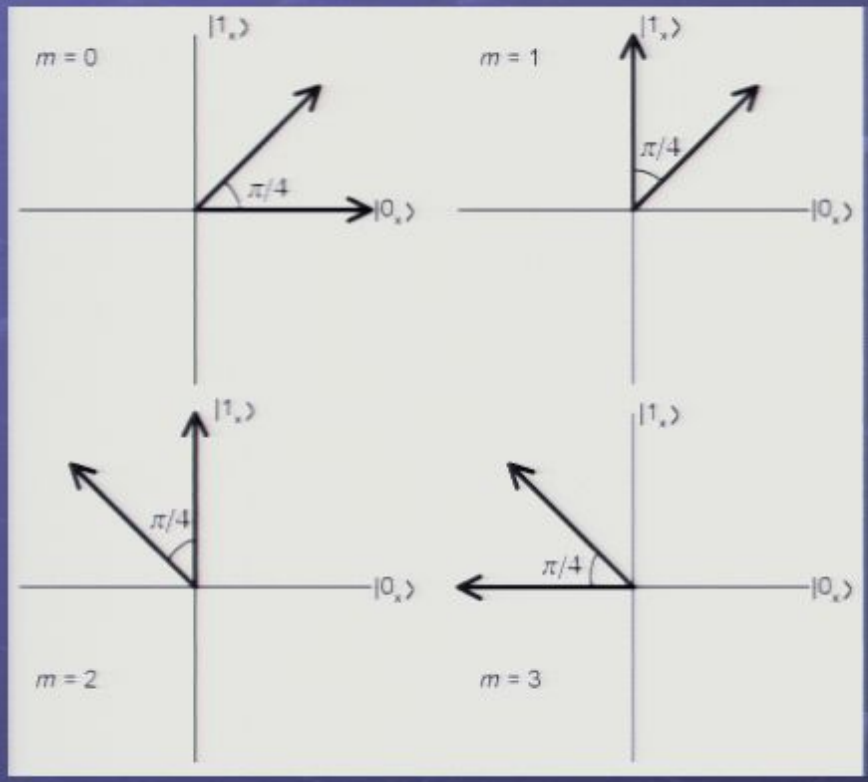
SARG04

- Unlike BB84, the two states in a basis in SARG04 are non-orthogonal



SARG04

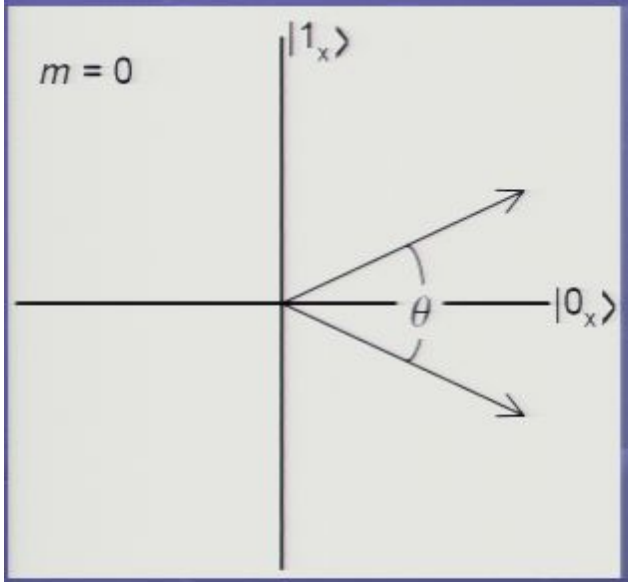
- Unlike BB84, the two states in a basis in SARG04 are non-orthogonal



- So, how do we detect the two non-orthogonal states?

How to detect non-orthogonal states

Alice Bob's projection Bob's decision

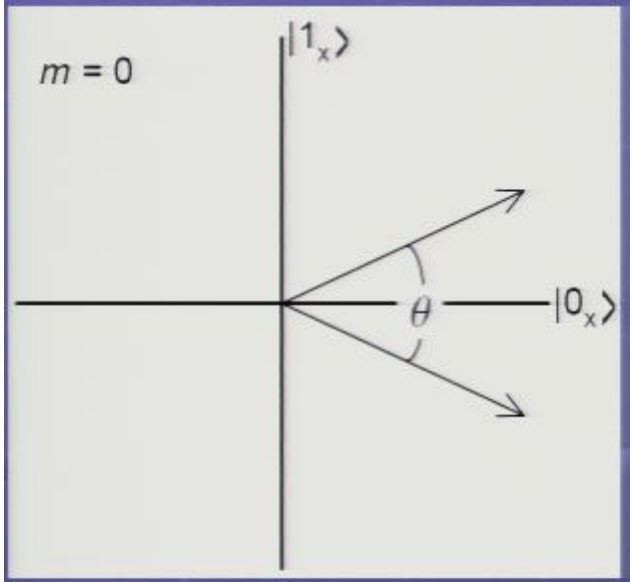


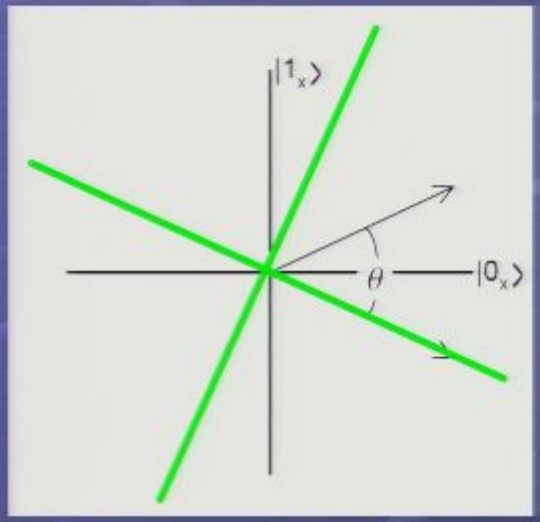
How to detect non-orthogonal states

Alice

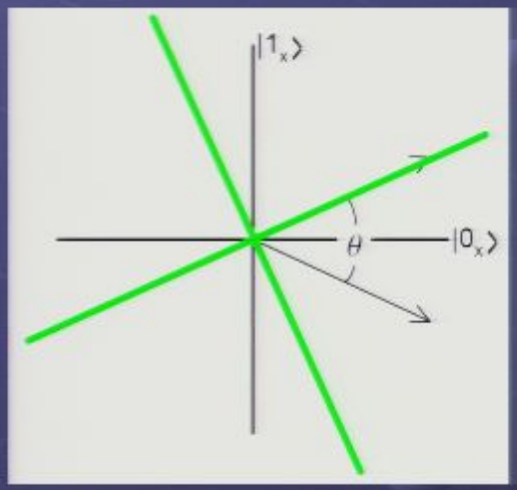
Bob's projection

Bob's decision





Prob = 1/2

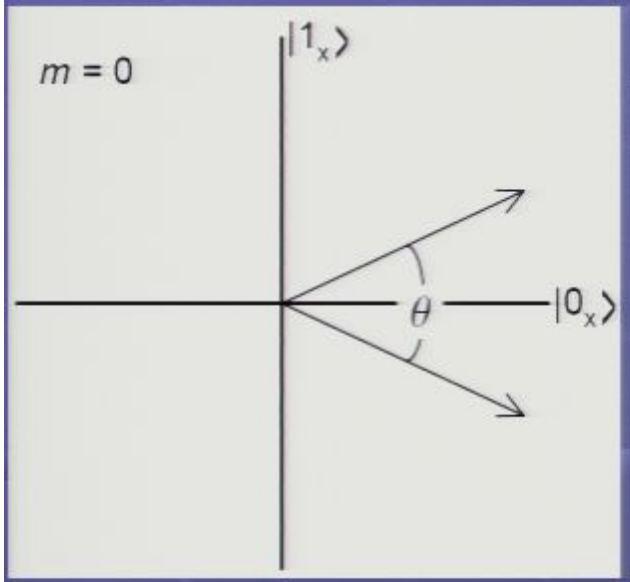


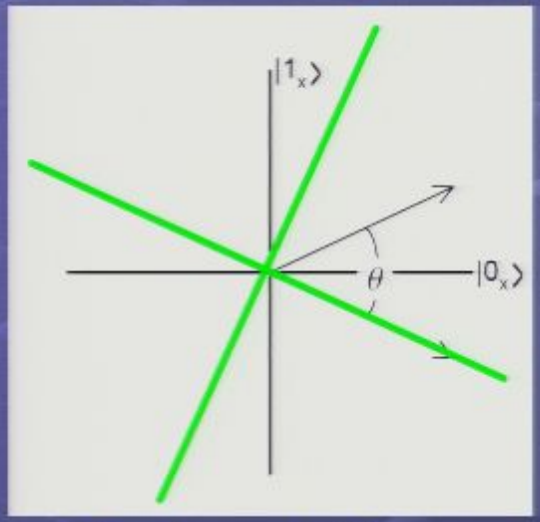
How to detect non-orthogonal states

Alice

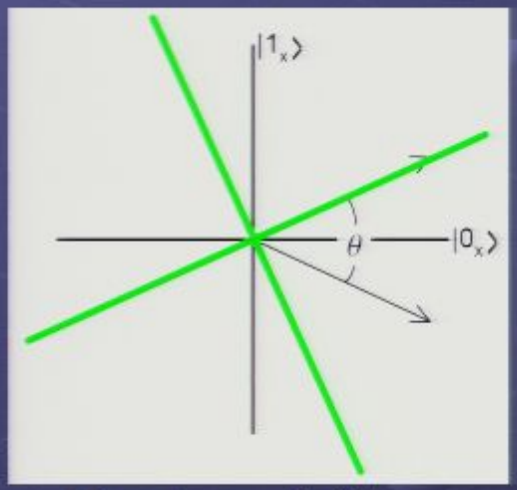
Bob's projection

Bob's decision





Prob = 1/2

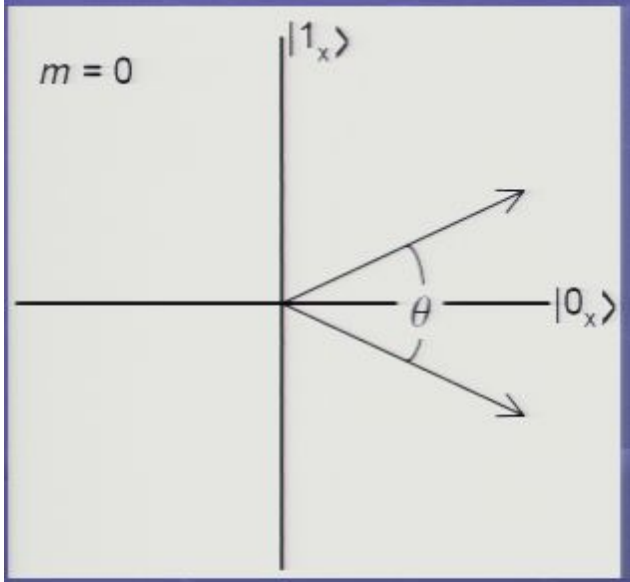


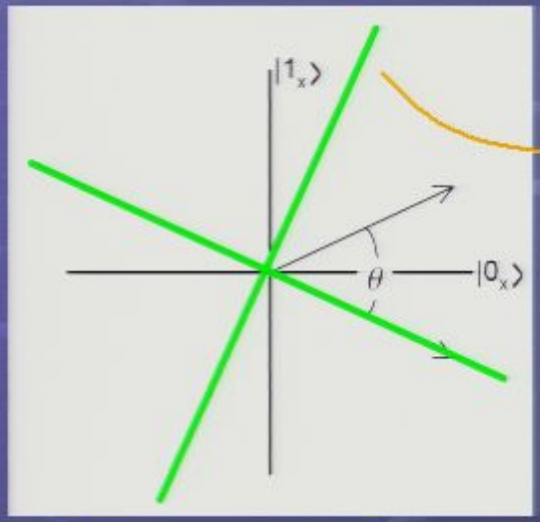
How to detect non-orthogonal states

Alice

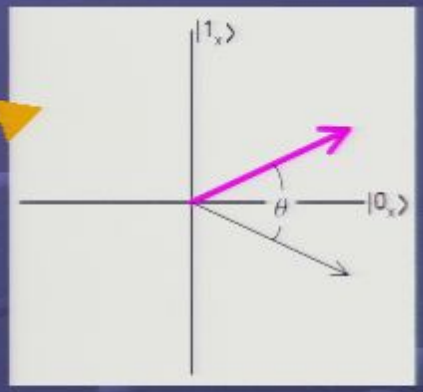
Bob's projection

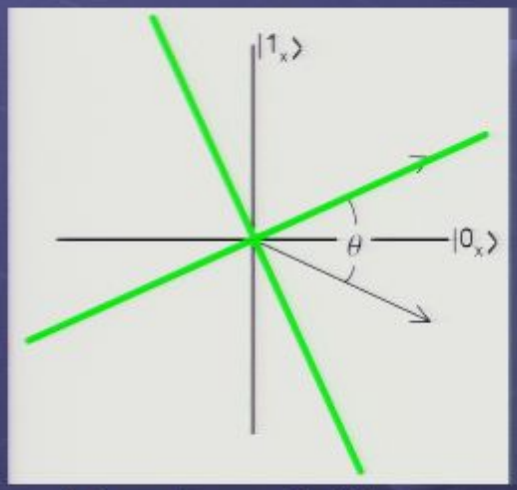
Bob's decision





Prob = 1/2



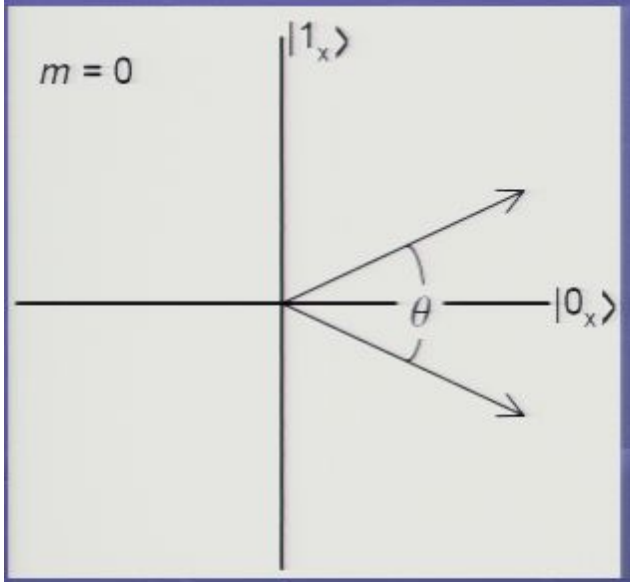


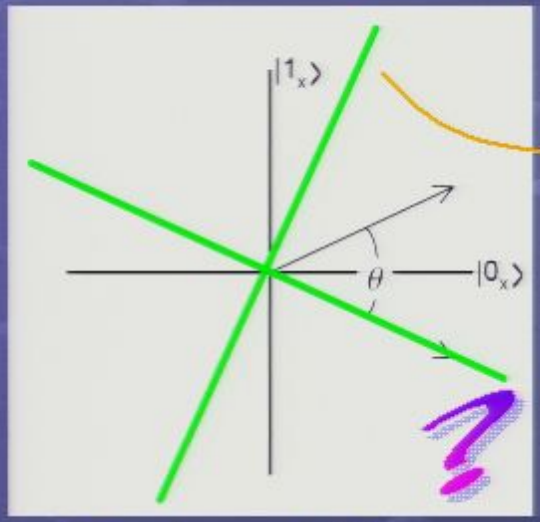
How to detect non-orthogonal states

Alice

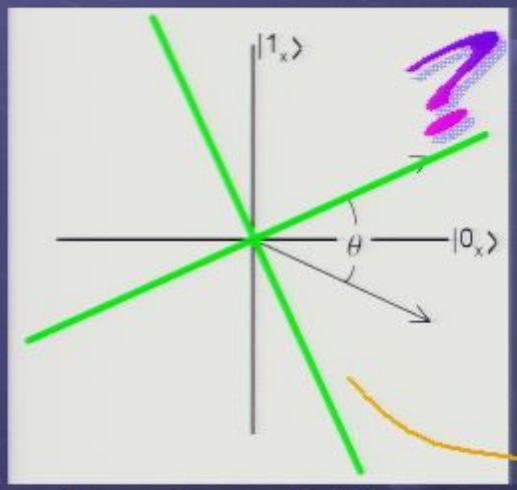
Bob's projection

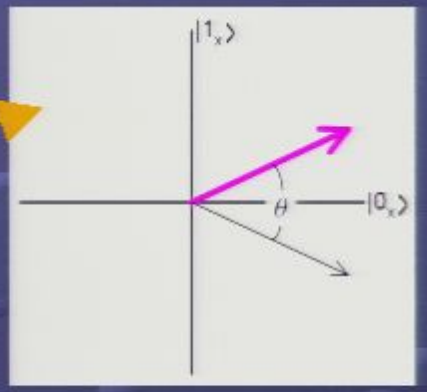
Bob's decision

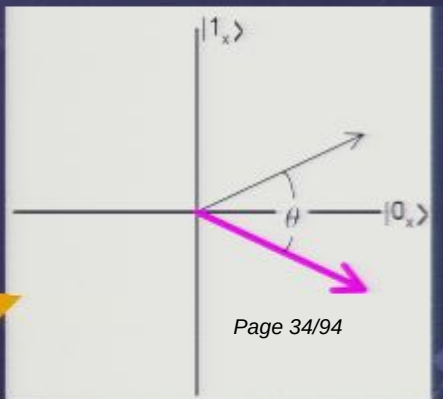




Prob = 1/2



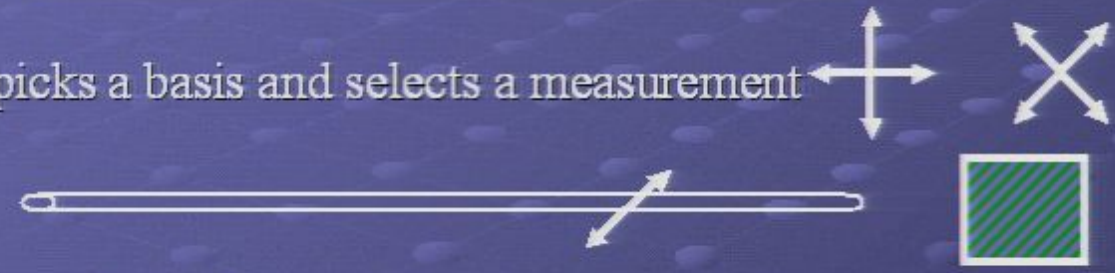




Procedure of generalized protocol (Sketch)

Step 1: Alice picks a basis and a state from it

Step 2: Bob picks a basis and selects a measurement



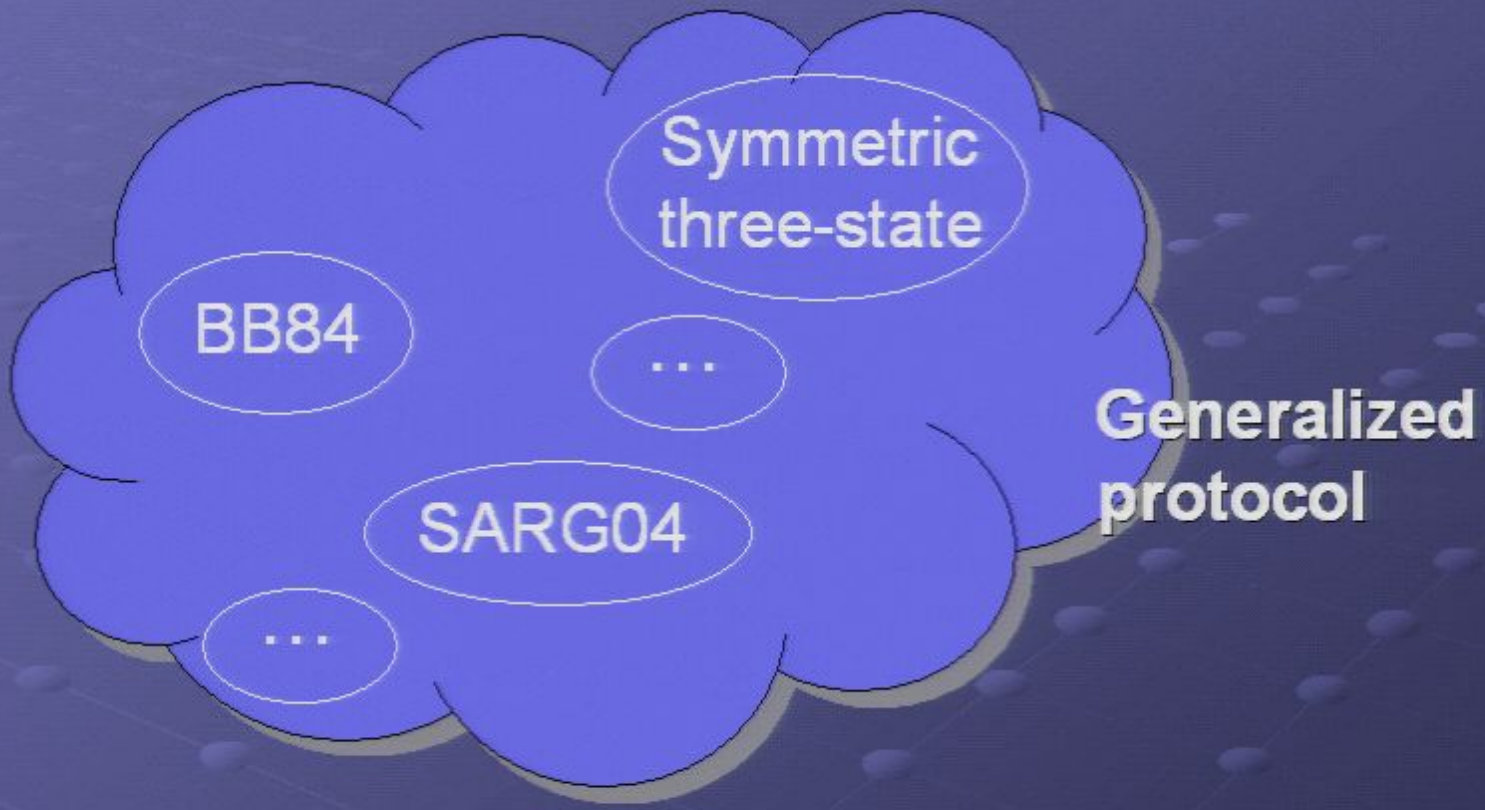
Step 3: Bob records his basis and measurement outcome.

measurement outcome decision

Step 4: Alice and Bob announce their bases publicly. They keep only the conclusive data for which they have used the same basis.

Step 5: Test for tampering by random sampling and computing quantum bit error rate. If error rate is OK, apply error correction and "privacy amplification".

Protocol 1: Generalized QKD Protocol



Goal: provide a unified security proof for QKD protocols with symmetry

Ideas of security proof

- Entanglement distillation picture [Lo-Chau and Shor-Preskill]

Ideas of security proof

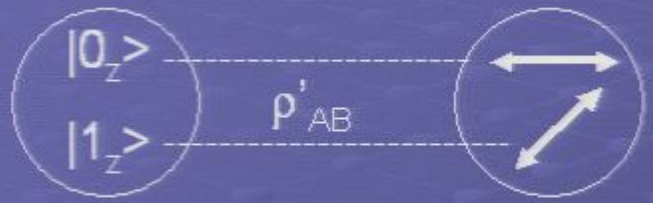
- Entanglement distillation picture [Lo-Chau and Shor-Preskill]

1. Alice's preparation

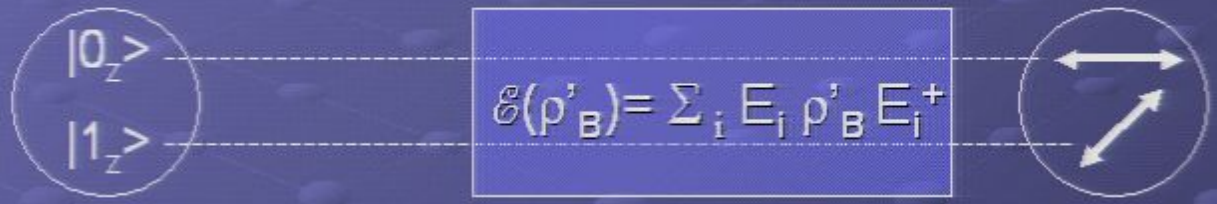
Ideas of security proof

- Entanglement distillation picture [Lo-Chau and Shor-Preskill]

1. Alice's preparation



2. Noisy channel (Eve)

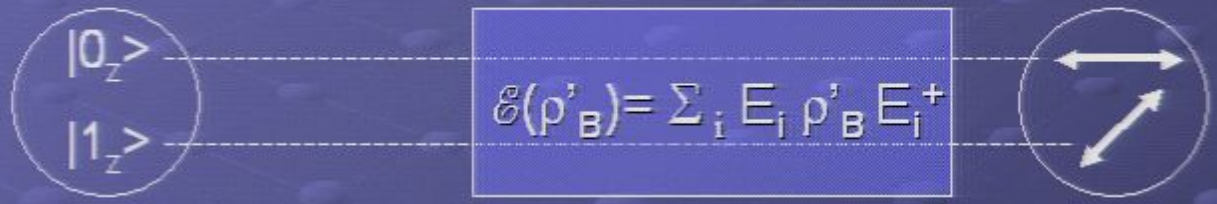


Ideas of security proof

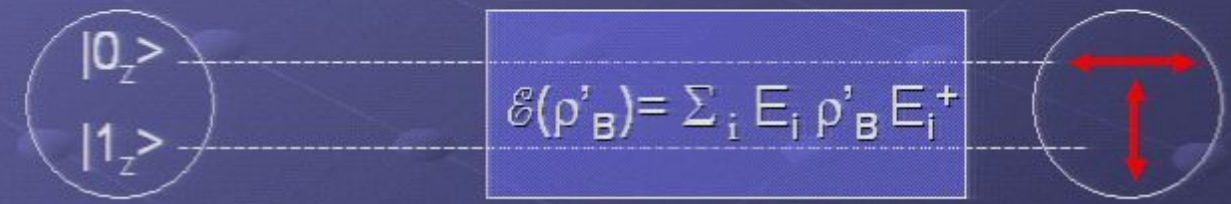
- Entanglement distillation picture [Lo-Chau and Shor-Preskill]

1. Alice's preparation

2. Noisy channel (Eve)



3. Bob's filtering (for detecting non-orthogonal states)



Final density matrix of Alice and Bob = ρ_{AB}

Ideas of security proof

[Lo and Chau, Science 283, 2050 (1999); Shor and Preskill, Phys. Rev. Lett. 85, 441 (2000).]

Ideas of security proof

- The idea of Lo-Chau and Shor-Preskill is to distill pure EPR pairs from ρ_{AB}

[Lo and Chau, Science 283, 2050 (1999); Shor and Preskill, Phys. Rev. Lett. 85, 441 (2000).]

Ideas of security proof

- The idea of Lo-Chau and Shor-Preskill is to distill pure EPR pairs from ρ_{AB}
- Initially treat the QKD protocol as an entanglement distillation protocol (EDP)

[Lo and Chau, Science 283, 2050 (1999); Shor and Preskill, Phys. Rev. Lett. 85, 441 (2000).]

Ideas of security proof

- The idea of Lo-Chau and Shor-Preskill is to distill pure EPR pairs from ρ_{AB}
- Initially treat the QKD protocol as an entanglement distillation protocol (EDP)
- Key point in Shor-Preskill is the reduction of the EDP to the QKD protocol

[Lo and Chau, Science 283, 2050 (1999); Shor and Preskill, Phys. Rev. Lett. 85, 441 (2000).]

Ideas of security proof

- The idea of Lo-Chau and Shor-Preskill is to distill pure EPR pairs from ρ_{AB}
- Initially treat the QKD protocol as an entanglement distillation protocol (EDP)
- Key point in Shor-Preskill is the reduction of the EDP to the QKD protocol
- The steps in an entanglement distillation protocol (EDP) become the error correction step and the privacy amplification step in the QKD protocol

[Lo and Chau, Science 283, 2050 (1999); Shor and Preskill, Phys. Rev. Lett. 85, 441 (2000).]

Ideas of security proof

otocol
dge on ρ_{AB}

Ideas of security proof

- In order to run an entanglement distillation protocol (EDP), Alice and Bob need to acquire knowledge on ρ_{AB}

Ideas of security proof

- In order to run an entanglement distillation protocol (EDP), Alice and Bob need to acquire knowledge on ρ_{AB}

- However, Alice and Bob do not in general know ρ_{AB} completely (no quantum computers)

Ideas of security proof

- In order to run an entanglement distillation protocol (EDP), Alice and Bob need to acquire knowledge on ρ_{AB}
- However, Alice and Bob do not in general know ρ_{AB} completely (no quantum computers)
- Fortunately, it is sufficient to know only the bit error rate and the phase error rate of ρ_{AB} to run the EDP

What are the bit and phase error rates?

- Express Alice and Bob's density matrix ρ_{AB} in the Bell basis

Bell basis: $$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_z, |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_z.$$

What are the bit and phase error rates?

- Express Alice and Bob's density matrix ρ_{AB} in the Bell basis

Bell basis: $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_z, |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_z.$

- Diagonal elements of ρ_{AB} become:

$$p_I = \langle \Phi^+ | \rho_{AB} | \Phi^+ \rangle \quad \text{(No error)}$$

$$p_x = \langle \Psi^+ | \rho_{AB} | \Psi^+ \rangle \quad \text{(Bit flip error)}$$

$$p_y = \langle \Psi^- | \rho_{AB} | \Psi^- \rangle \quad \text{(Bit flip and phase flip error)}$$

$$p_z = \langle \Phi^- | \rho_{AB} | \Phi^- \rangle \quad \text{(Phase flip error)}$$

Bit error: $|0_z\rangle \rightarrow |1_z\rangle$, $|1_z\rangle \rightarrow |0_z\rangle$

Phase error: $|1_+\rangle \rightarrow -|1_-\rangle$

What are the bit and phase error rates?

$$p_I = \langle \Phi^+ | \rho_{AB} | \Phi^+ \rangle$$ (No error)

$$p_x = \langle \Psi^+ | \rho_{AB} | \Psi^+ \rangle$$ (Bit flip error)

$$p_y = \langle \Psi^- | \rho_{AB} | \Psi^- \rangle$$ (Bit flip and phase flip error)

$$p_z = \langle \Phi^- | \rho_{AB} | \Phi^- \rangle$$ (Phase flip error)

e_b = Bit error rate = $p_x + p_y$

e_p = Phase error rate = $p_z + p_y$

Bit and phase error rates

error rate is
in general

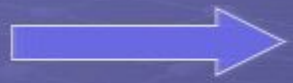
Bit and phase error rates

No Quantum Computer

Only the bit error rate is measurable in general

Bit and phase error rates

No Quantum Computer



Only the bit error rate is measurable in general

But, we need both the bit error rate and the phase error rate in order to run an EDP

Bit and phase error rates

No Quantum Computer → Only the bit error rate is measurable in general

But, we need both the bit error rate and the phase error rate in order to run an EDP

→ Need to infer the phase error rate from the bit error rate

Bit and phase error rates

No Quantum Computer → Only the bit error rate is measurable in general

But, we need both the bit error rate and the phase error rate in order to run an EDP

→ Need to infer the phase error rate from the bit error rate

Goal: Find phase and bit error rate relation

$$e_p = f(e_b)$$

Protocol Security

phase and bit error rate relation

$e_p = f(e_b)$

Single-photon source

Coherent-light source

Shor-Preskill's argument

Shor and Preskill, PRL 85, 441 (2000)

GLLP's argument

Gottesman, Lo, Lütkenhaus, and Preskill, QIC 5, 325 (2004)

Unconditional security

Generalized Protocol: Phase and bit error rate relation

$$e_p = e_b (1+\cos^2 \theta) \quad (M>2)$$

- e_p is the phase error rate averaged over all M bases
- e_b is the bit error rate averaged over all M bases
- θ is the angle between the basis states
- Independent of the number of bases, M (for M > 2)

Generalized Protocol

Spherical averages → Simple relation between e_p and e_b

$$
\begin{aligned}
p_x &= \langle \Phi^- | \rho_{AB} | \Phi^- \rangle \\
&= \frac{1}{M} \sum_j \sum_{l=0}^{M-1} \left| \langle \Phi^- | \hat{I}_A \otimes (\hat{F}_0 \hat{R}_{-l\pi/M} \hat{E}_j \hat{R}_{l\pi/M})_B | \psi \rangle_{AB} \right|^2 \\
&= \frac{1}{M} \sum_{l=0}^{M-1} \left| \frac{1}{\sqrt{2}} (\langle 00| - \langle 11|) \otimes (\hat{F}_0 \hat{R}_{-l\pi/M} \hat{E}_j \hat{R}_{l\pi/M})_B \right. \\
&\quad \left. (\cos\frac{\theta}{2}|00\rangle_B + \sin\frac{\theta}{2}|11\rangle) \right|^2 \\
&= \frac{\sin^2\theta}{4M} \sum_{l=0}^{M-1} |\langle 0| \hat{R}_{-l\pi/M} \hat{E}_j \hat{R}_{l\pi/M} |0\rangle - \langle 1| \hat{R}_{-l\pi/M} \hat{E}_j \hat{R}_{l\pi/M} |1\rangle|^2 \\
&= \cdots \frac{1}{M} \sum_{l=0}^{M-1} \cos^2 kl\pi/M \cdots \quad \frac{1}{M} \sum_{l=0}^{M-1} \sin^2 kl\pi/M \cdots
\end{aligned}
$$

1/2 1/2

(M > 2)

Comparison with previous results

Protocols

Bit/phase error rate relations

General formula

$$e_p = e_b (1+\cos^2 \theta)$$

Comparison with previous results

Protocols

Bit/phase error rate relations

BB84

M=4 and $\theta=\pi/2$

$e_p = e_b$

[Lo and Chau, Science 283, 2050 (1999); Shor and Preskill, PRL 85, 441 (2000).]

General formula

$$e_p = e_b (1+\cos^2 \theta)$$

Comparison with previous results

Protocols

Bit/phase error rate relations

BB84

M=4 and $\theta=\pi/2$

$e_p = e_b$

[Lo and Chau, Science 283, 2050 (1999); Shor and Preskill, PRL 85, 441 (2000).]

General formula

$e_p = e_b (1+\cos^2 \theta)$

SARG04

M=4 and $\theta=\pi/4$

$e_p = (3/2)\, e_b$

[Tamaki and Lo, PRA 73, 010302 (2006); Fung, Tamaki, and Lo, PRA 73 012337 (2006).]

Comparison with previous results

Protocols

Bit/phase error rate relations

BB84

M=4 and $\theta=\pi/2$

SARG04

M=4 and $\theta=\pi/4$

Symmetric three-state

M=3 and $\theta=\pi/3$

General formula

$$e_p = e_b (1+\cos^2 \theta)$$

$e_p = e_b$

[Lo and Chau, Science 283, 2050 (1999); Shor and Preskill, PRL 85, 441 (2000).]

$e_p = (3/2)\, e_b$

[Tamaki and Lo, PRA 73, 010302 (2006); Fung, Tamaki, and Lo, PRA 73 012337 (2006).]

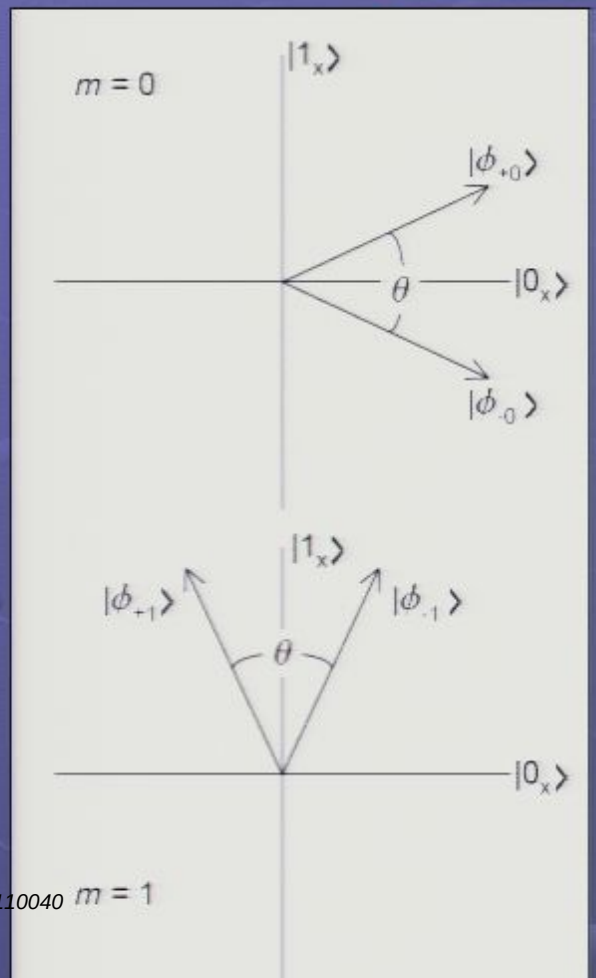
$e_p = (5/4)\, e_b$

[Boileau, et al., PRL 94, 040503 (2005).]

Generalized Protocol

$$e_p \leq \frac{1+\cos^2\theta}{\cos^2\theta}\, e_b$$

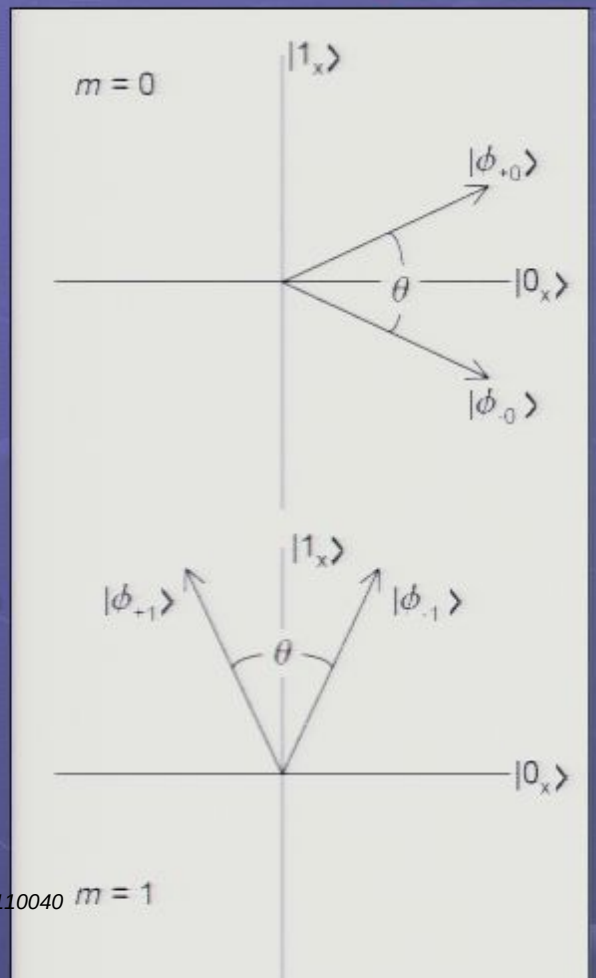
(M=2)



Generalized Protocol

$$e_p \leq \frac{1+\cos^2\theta}{\cos^2\theta}\, e_b$$

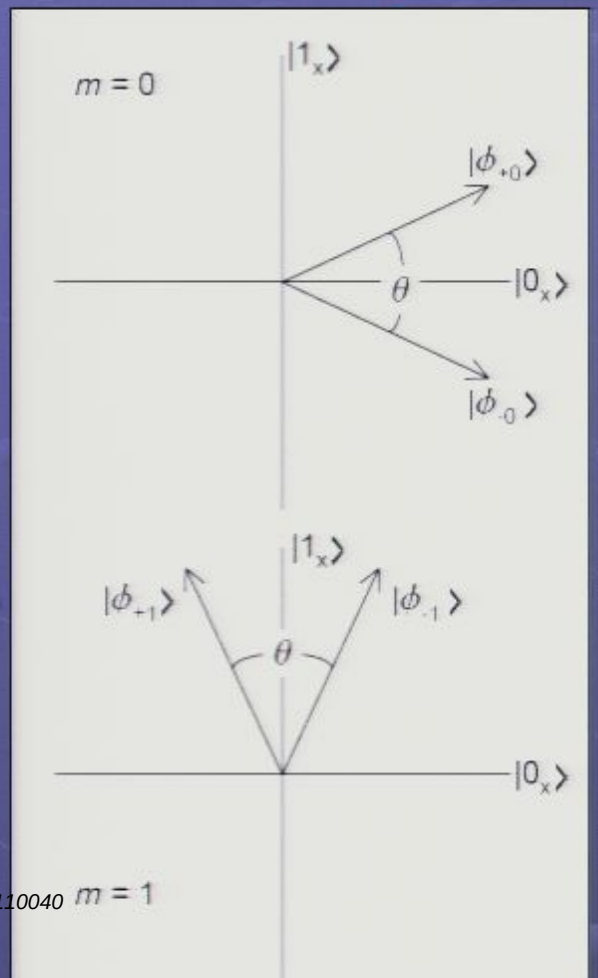
(M=2)



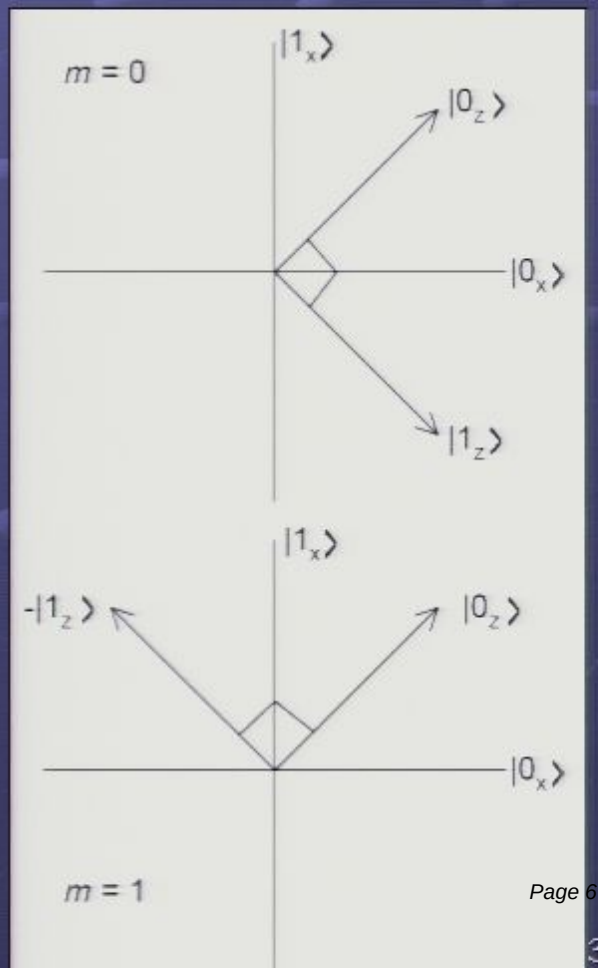
$\theta=\pi/2$

Generalized Protocol

$$e_p \leq \frac{1+\cos^2\theta}{\cos^2\theta}\, e_b \qquad (M=2)$$



$\theta=\pi/2$



Lesson 1: rotational symmetry

- Discrete rotational symmetry in the QKD protocol simplifies the effect of a noisy channel or an eavesdropper and has the same effect as continuous symmetry.

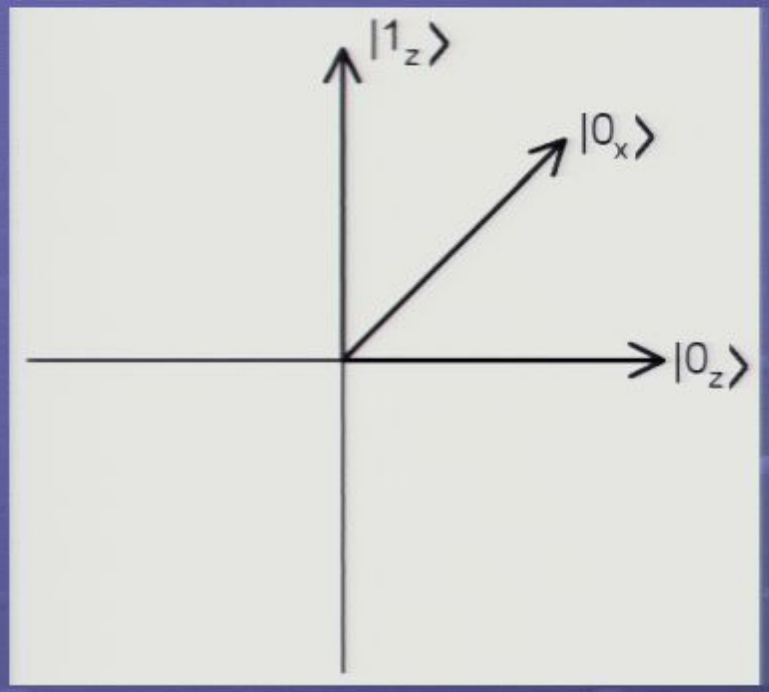
- This results in a simple relationship between the bit and phase error rates as a function of the angle between the basis states θ, but not of the number of bases M>2.

$$e_p = e_b (1+\cos^2 \theta)$$

Outline

- Introduction to QKD protocols
- Motivation for studying rotational symmetry in QKD protocols
- Protocol 1: Generalized QKD protocol
- Protocol 2: Three-state protocol
- Secret key generation rate
  - Single-photon source
  - Coherent light source
- Conclusion

Protocol 2: A three-state protocol



- Alice sends one of { $|0_z\rangle$, $|1_z\rangle$, $|0_x\rangle$ }
- $|0_z\rangle$ and $|1_z\rangle$ for key generation
- $|0_x\rangle$ for channel estimation
- Similar to BB84 *except without rotational symmetry*

Three-state protocol: Applications

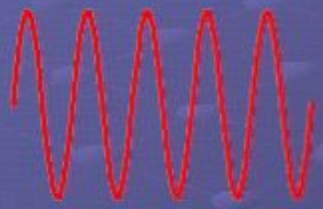
Three-state protocol: Applications

1. Frequency-based QKD system

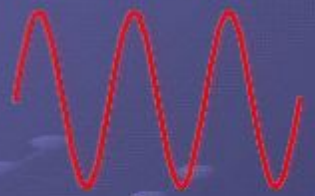
[N. Molotkov et al., J. Exp. and Theo. Phys. Lett. 63, 924 (1996); Shi et al., Appl. Phys. B 70, 415 (2000)]

$|0_z\rangle$ =

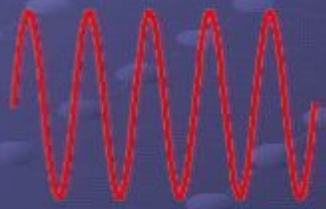
$|1_z\rangle$ =



$|0_x\rangle$ =



+



Three-state protocol: Applications

1. Frequency-based QKD system

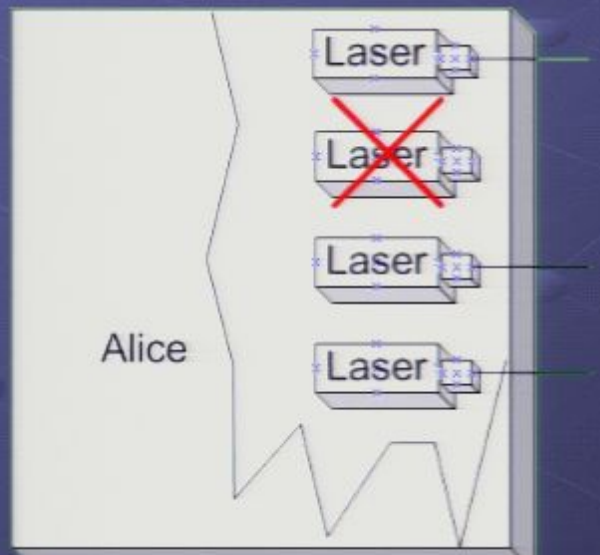
[N. Molotkov et al., J. Exp. and Theo. Phys. Lett. 63, 924 (1996); Shi et al., Appl. Phys. B 70, 415 (2000)]

$|0_z\rangle$ =

$|1_z\rangle$ =

$|0_x\rangle$ = +

2. Broken laser in BB84



Can we prove security when there is no symmetry?

Can we prove security when there is no symmetry?

YES!

Can we prove security when there is no symmetry?

YES!

- We derive the relation between bit and phase error rates:

Max	e_p(Eve's attack)
s.t.	e_b(Eve's attack) = observed bit error rate in $\|0_z\rangle$, $\|1_z\rangle$
	α (Eve's attack) = observed bit error rate in $\|0_x\rangle$

- α : bit error rate in $|0_x\rangle$
- e_b (e_p) : bit (phase) error rate in $|0_z\rangle$ and $|1_z\rangle$

Three-state protocol without rotational symmetry

Three-state protocol without rotational symmetry

- We do not get nice spherical averages that simplify the problem
- Nevertheless, we can still upper bound the phase error rate as

Three-state protocol without rotational symmetry

- We do not get nice spherical averages that simplify the problem
- Nevertheless, we can still upper bound the phase error rate as

$$e_p \leq \alpha + e_b(2 - 2\alpha - \alpha^2) + 2\sqrt{\alpha(1-\alpha)e_b(1 - e_b - e_b\alpha)}$$

- α : bit error rate in $|0_x\rangle$
- e_b (e_p) : bit (phase) error rate in $|0_z\rangle$ and $|1_z\rangle$

Lesson 2: no symmetry

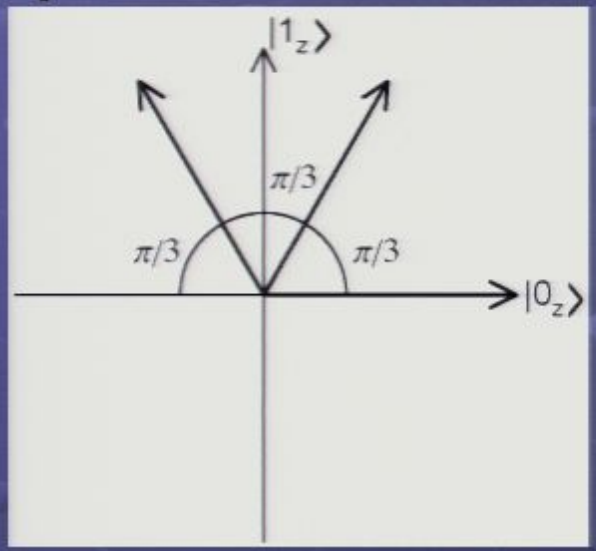
- Security can still be proven even *without* rotational symmetry.
- But, the relation between bit and phase error rates is more complicated.
  - Not linear

Related work (generalized protocol)

- Koashi [quant-ph/0507154] also studied a generalized QKD protocol similar to ours.
- However, in his protocol, there is an additional constraint that θ has to be some integer multiple of M/π, whereas we allow θ to be *arbitrary*.
- On the other hand, Koashi studied the multi-photon case as well

Related work (three-state protocol)

- Boileau, et al. [PRL 94, 040503 (2005)] proved the security of a *symmetric* three-state protocol



- A specific case of our generalized protocol (M=3, $\theta=\pi/3$)

Outline

- Introduction to QKD protocols
- Motivation for studying rotational symmetry in QKD protocols
- Protocol 1: Generalized QKD protocol
- Protocol 2: Three-state protocol
- Secret key generation rate
  - Single-photon source
  - Coherent light source
- Conclusion

Secret key generation rate: Single-photon source

- Using Shor-Preskill's argument, the secret key generation rate on the sifted key is

$$R = 1 - H_2(e_b) - H_2(e_p)$$

Generalized protocol

$$e_p = e_b\,(1+\cos^2\theta)$$

Three-state protocol

$$e_p \le \alpha + e_b(2-2\alpha-\alpha^2) + 2\sqrt{\alpha(1-\alpha)e_b(1-e_b-e_b\alpha)}$$

- where $H_2(x) = -x \log(x) - (1-x)\log(1-x)$ is the binary entropy function

Secret key generation rate: Coherent-light source

- Using GLLP's argument, the secret key generation rate is

$$R = - Q_{\mu} f(E_{\mu}) H_2(E_{\mu}) + Q_1 [1- H_2(e_p)]$$

- Q_{μ} : gain of the signal states
- E_{μ} : bit error rate of signal states
- Q_1 : gain of the single-photon states
- e_p : phase error rate of the single-photon states
- $H_2(\cdot)$: binary entropy function
- $f(E_{\mu})$: error correction efficiency

GLLP formula

$$R = - Q_{\mu} f(E_{\mu}) H_2(E_{\mu}) + Q_1 [1- H_2(e_p)]$$

Directly estimated

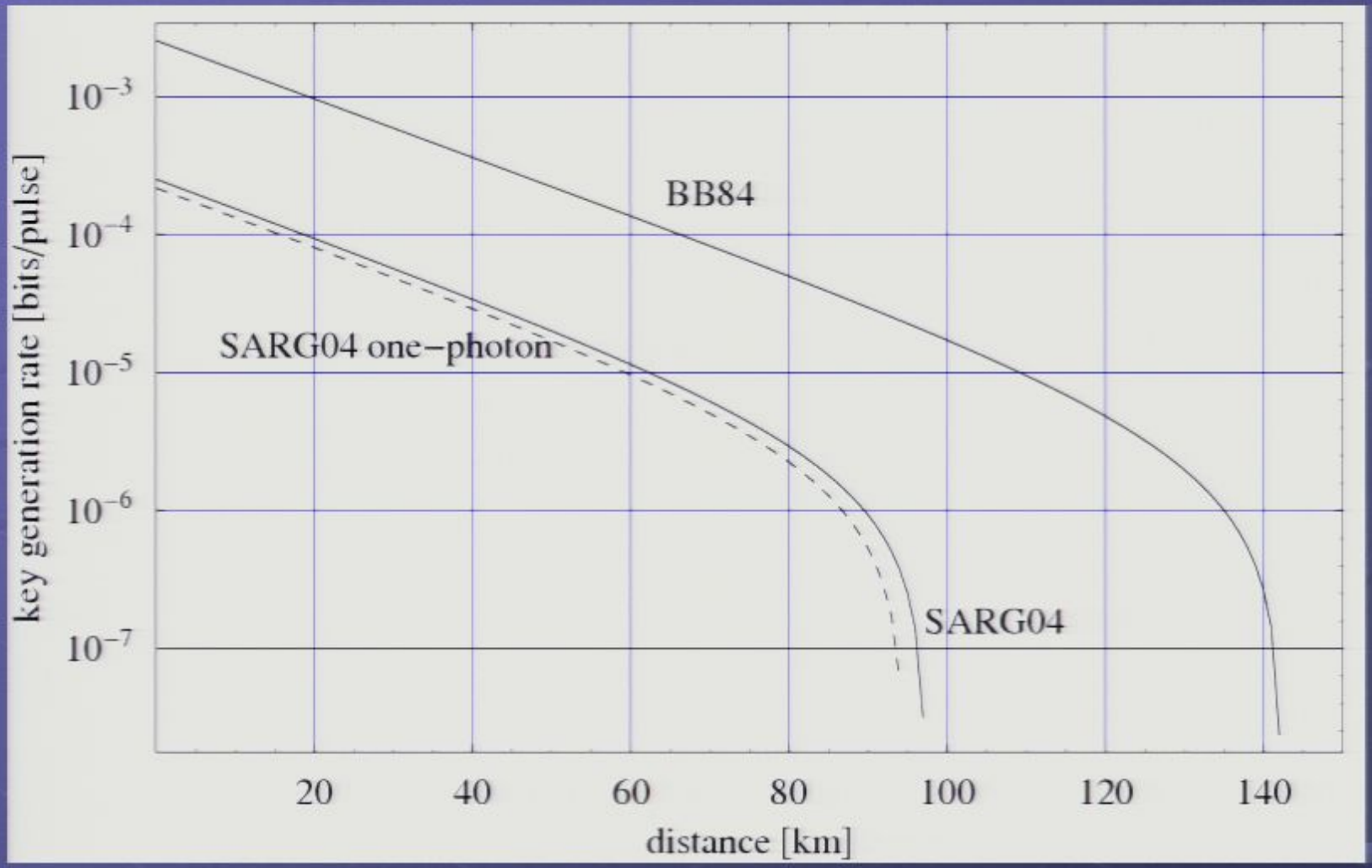
$e_p = f(e_b)$

Bit error rate(s) for single-photon states

Decoy-state method
[Lo, Ma, and Chen PRL 94, 230504 (2005); Hwang PRL 92, 057901 (2003); Wang PRL 94 230503 (2005); Harrington et al. (2005)]

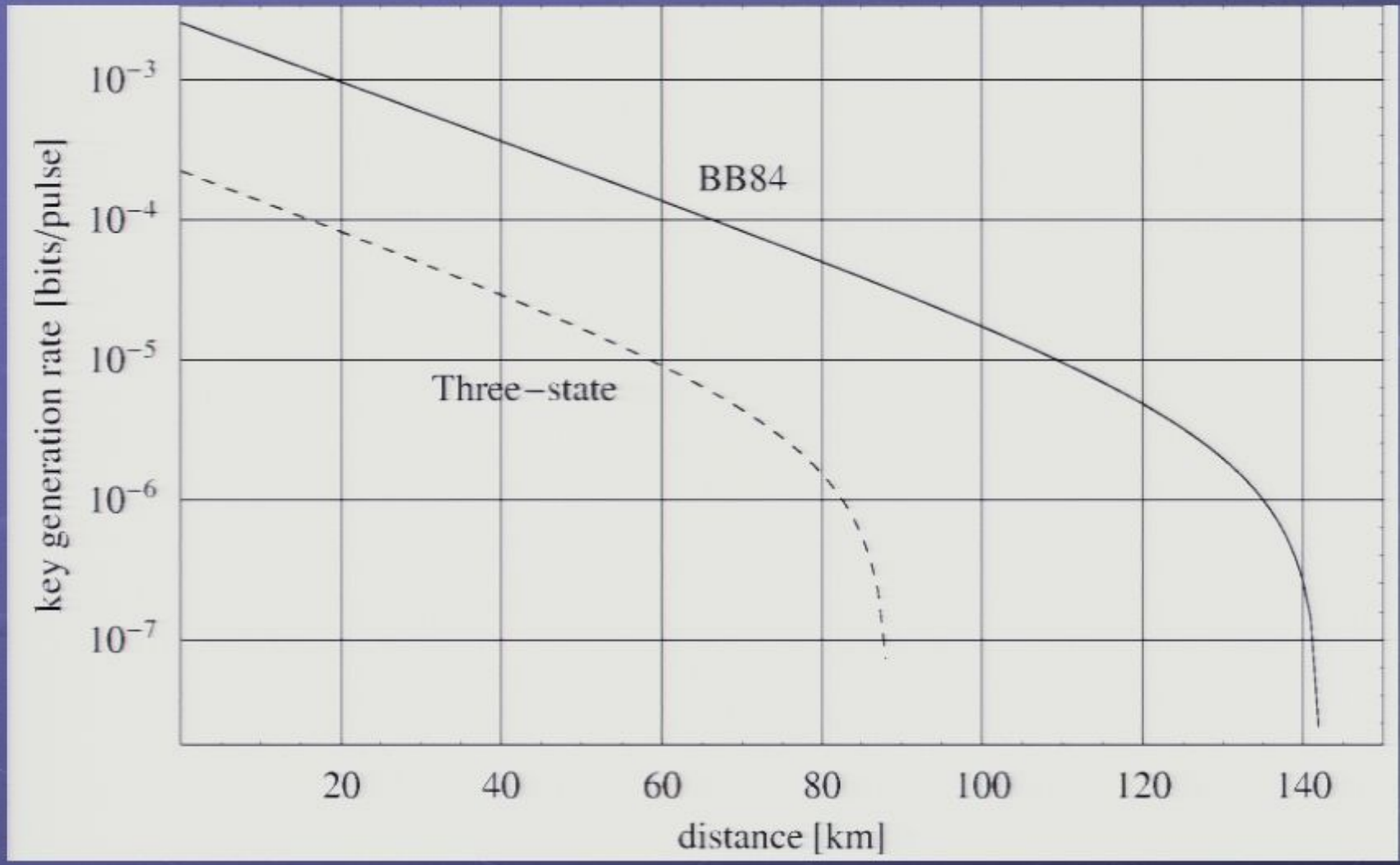
[Gottesman, Lo, Lütkenhaus, and Preskill, QIC 5, 325 (2004)]

Generalized protocol: Simulation



Simulation parameters from [Gobby, Yuan, and Shields APL 84, 3762 (2004)] and $f(E_\mu) = 1.22$

Asymmetric three-state protocol: Simulation



Simulation parameters from [Gobby, Yuan, and Shields APL 84, 3762 (2004)] and $f(E_\mu) = 1.22$

Outline

- Introduction to QKD protocols
- Motivation for studying rotational symmetry in QKD protocols
- Protocol 1: Generalized QKD protocol
- Protocol 2: Three-state protocol
- Secret key generation rate
  - Single-photon source
  - Coherent light source
- Conclusion

Conclusion

- Explored role of rotational symmetry of QKD protocols
- Proved the security of the generalized protocol (with symmetry) and the three-state protocol (no symmetry)
- Rotational symmetry
  - Simplifies security analysis
  - Leads to simple bit/phase error rate relation
- No rotational symmetry
  - Security can still be proven
  - Complicated bit/phase error rate relation
- Open problem: multi-photon for the generalized protocol

Our Contributions

- Generalized protocol:
  D. Shirokoff, C.-H. F. Fung, and H.-K. Lo, "Discrete rotational symmetry and quantum key distribution", quant-ph/0604198.

- Three-state protocol without rotational symmetry:
  C.-H. F. Fung and H.-K. Lo, "Security proof of a three-state quantum-key-distribution protocol without rotational symmetry ", Phys. Rev. A 74, 042342 (2006).

References

1. D. Mayers, J. of ACM 48, 351 (2001).
2. N. Lütkenhaus, Phys. Rev. A 61, 052304, (2000).
3. H.-K. Lo and H. F. Chau, Science 283, 2050 (1999)
4. P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
5. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Info. and Comp. 4, 325 (2004).
6. W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
7. X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005); Phys. Rev. A72, 012322 (2005).
8. J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, quant-ph/0503002.
9. K. Tamaki and H.-K. Lo, Phys. Rev. A 73, 010302 (2006).
10. C.-H. F. Fung, K. Tamaki, and H.-K. Lo, Phys. Rev. A 73 012337 (2006).
11. J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. 94, 040503 (2005).
12. C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. 84, 3762 (2004).

Thanks!

NSERC CRSNG

Canada Research Chairs

ICIP CIPI

CIAR Canadian Institute for Advanced Research

Ontario Innovation Trust

premier's research excellence awards

Canada Foundation for Innovation
Fondation canadienne pour l'innovation

Ontario OGSST

Walter C. Sumner Memorial Fellowships

MITACS

Secret key generation rate: Single-photon source

- Using Shor-Preskill's argument, the secret key generation rate on the sifted key is

$$R = 1 - H_2(e_b) - H_2(e_p)$$

Generalized protocol

$$e_p = e_b\,(1+\cos^2\theta)$$

Three-state protocol

$$e_p \le \alpha + e_b(2 - 2\alpha - \alpha^2) + 2\sqrt{\alpha(1-\alpha)e_b(1 - e_b - e_b\alpha)}$$

- where $H_2(x) = -x \log(x) - (1-x) \log(1-x)$ is the binary entropy function