

Quantum key distribution for the lazy and careless

Noisy preprocessing and twisted states

Joseph M. Renes



Theoretical Quantum Physics, Institut für Angewandte Physik
Technische Universität Darmstadt

Center for Advanced Studies Seminar
University of New Mexico
2006 October 26



Outline

- 1 Quantum Key Distribution
 - Prepare & Measure QKD
 - BB84 — The canonical protocol
- 2 Security of QKD
 - Assured Privacy from Provable Entanglement
 - Key Distillation from Entanglement Distillation
- 3 Preprocessing & Twisted States
 - Noisy Preprocessing
 - Twisted States
 - Degenerate Code-based Preprocessing



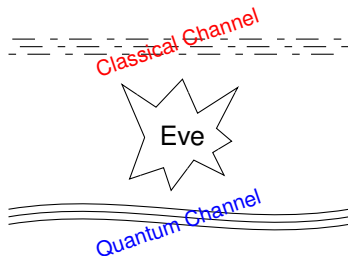
Key Distribution Setup

Goal: *expand* authentication key to a size useful for data encryption

(key *distribution* is a misnomer)



Alice



Bob

- Parties can **prepare** and **measure** individual systems
- Transmit over an insecure quantum channel
- Use *authenticated* classical broadcast channel

Quantum Key Distribution Schemes

Bennett Brassard 1984 (BB84)

Original scheme — prepare & measure x and z basis states

Ekert 1991 (E91)

- ♣ Based on Bell inequality violation
- ♣ No need for Hilbert space

Bennett 1992 (B92)

- ♥ Just two nonorthogonal states
- ♥ Information-disturbance tradeoff

Phoenix, Barnett, Chefles 2000 & Yours truly 2004

- ♦ QKD with spherical codes
- ♦ New signal → key decoding methods

Scarani, Acín, Ribordy, Gisin 2004 (SARG04)

- ♠ BB84 signals, decoded differently
- ♠ Resists channel loss



The BB84 Protocol: Basics



- 1 Alice sends random signals from the set
- 2 Bob randomly measures in the Z or X bases
- 3 Both parties announce their bases
- 4 Keep data corresponding to the same basis
- 5 Relabel:

The BB84 Protocol: Basics



- 1 Alice sends random signals from the set $\{\uparrow, \downarrow, \rightarrow, \leftarrow\}$
- 2 Bob randomly measures in the Z or X bases
- 3 Both parties announce their bases
- 4 Keep data corresponding to the same basis
- 5 Relabel:

The BB84 Protocol: Basics



- 1 Alice sends random signals from the set $\{\uparrow, \downarrow, \rightarrow, \leftarrow\}$
- 2 Bob randomly measures in the Z or X bases
- 3 Both parties announce their bases
- 4 Keep data corresponding to the same basis
- 5 Relabel:

The BB84 Protocol: Basics



- 1 Alice sends random signals from the set $\{\uparrow, \downarrow, \rightarrow, \leftarrow\}$
- 2 Bob randomly measures in the **Z** or **X** bases
- 3 Both parties announce their bases
- 4 Keep data corresponding to the same basis
- 5 Relabel:

The BB84 Protocol: Basics



- 1 Alice sends random signals from the set $\{\uparrow, \downarrow, \rightarrow, \leftarrow\}$
- 2 Bob randomly measures in the **Z** or **X** bases
- 3 Both parties announce their bases
- 4 Keep data corresponding to the same basis
- 5 Relabel:

The BB84 Protocol: Basics



X Z Z X Z



X Z X Z Z



- 1 Alice sends random signals from the set $\{\uparrow, \downarrow, \rightarrow, \leftarrow\}$
- 2 Bob randomly measures in the Z or X bases
- 3 Both parties announce their bases
- 4 Keep data corresponding to the same basis
- 5 Relabel:

The BB84 Protocol: Basics



X Z Z X Z



X Z X Z Z



- 1 Alice sends random signals from the set $\{\uparrow, \downarrow, \rightarrow, \leftarrow\}$
- 2 Bob randomly measures in the Z or X bases
- 3 Both parties announce their bases
- 4 Keep data corresponding to the same basis
- 5 Relabel:

The BB84 Protocol: Basics



X Z Z X Z

0 1 ↑ ← 0

X Z X Z Z

0 1 ← ↓ 0



- 1 Alice sends random signals from the set $\{\uparrow, \downarrow, \rightarrow, \leftarrow\}$
- 2 Bob randomly measures in the Z or X bases
- 3 Both parties announce their bases
- 4 Keep data corresponding to the same basis
- 5 Relabel: $\{\uparrow, \rightarrow\} \rightarrow 0, \{\downarrow, \leftarrow\} \rightarrow 1$

BB84 Protocol: Entangled version

Alice can send random signals by:

- 1 Preparing the state $|\Phi\rangle_{AB} = |\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle = |\rightarrow\rightarrow\rangle + |\leftarrow\leftarrow\rangle$
- 2 Sending the second half to Bob
- 3 Randomly measuring her half in the **X** and **Z** bases

☞ Two protocols are identical from the outside:

- ☞ One photon is transmitted
- ☞ Public information identical

☞ But the key *doesn't exist* until after transmission!

- ☞ Polarization state of photon not well-defined

☞ *Virtual entanglement* ensures the privacy of the key in prepare & measure BB84

BB84 Protocol: Entangled version

Alice can send random signals by:

- 1 Preparing the state $|\Phi\rangle_{AB} = |\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle = |\rightarrow\rightarrow\rangle + |\leftarrow\leftarrow\rangle$
- 2 Sending the second half to Bob
- 3 Randomly measuring her half in the **X** and **Z** bases

👉 Two protocols are identical from the outside:

- 👉 One photon is transmitted
- 👉 Public information identical

👉 But the key *doesn't exist* until after transmission!

- 👉 Polarization state of photon not well-defined

👉 *Virtual entanglement* ensures the privacy of the key in prepare & measure BB84

QKD Security: Entanglement Cannot be Shared

Alice and Bob do not know what (virtual) state they share.

💡 Sacrifice some key bits to find out! (Assume i.i.d. state)

Suppose test reports no errors

- 🔍 Their test is a measurement of $X_A \otimes X_B$ and $Z_A \otimes Z_B$
- 🔍 Eve hasn't caused any disturbance to the state

🔍 Consistent quantum state:

$$\left. \begin{aligned} X_A \otimes X_B &= +1 \\ Z_A \otimes Z_B &= +1 \end{aligned} \right\} \Rightarrow |\Phi\rangle_{AB}$$

- 🔍 Keys described by $|\Phi\rangle$ are secret, since the $\rho_{ABE} = \Phi_{AB} \otimes \rho_E$
Eve is completely uncorrelated with the key

QKD Security: Entanglement Cannot be Shared

Alice and Bob do not know what (virtual) state they share.

💡 Sacrifice some key bits to find out! (Assume i.i.d. state)

Suppose test reports no errors

- 👉 Their test is a measurement of $X_A \otimes X_B$ and $Z_A \otimes Z_B$
- 👉 Eve hasn't caused any disturbance to the state

👉 Consistent quantum state:

$$\left. \begin{aligned} X_A \otimes X_B &= +1 \\ Z_A \otimes Z_B &= +1 \end{aligned} \right\} \Rightarrow |\Phi\rangle_{AB}$$

👉 Keys described by $|\Phi\rangle$ are secret, since the $\rho_{ABE} = \Phi_{AB} \otimes \rho_E$
Eve is completely uncorrelated with the key

QKD Security: Entanglement Cannot be Shared

Alice and Bob do not know what (virtual) state they share.

💡 Sacrifice some key bits to find out! (Assume i.i.d. state)

Suppose test reports no errors

👉 Their test is a measurement of $X_A \otimes X_B$ and $Z_A \otimes Z_B$

👉 Eve hasn't caused any disturbance to the state

👉 Consistent quantum state:

$$\left. \begin{aligned} X_A \otimes X_B &= +1 \\ Z_A \otimes Z_B &= +1 \end{aligned} \right\} \Rightarrow |\Phi\rangle_{AB}$$

👉 **Keys described by $|\Phi\rangle$ are secret**, since the $\rho_{ABE} = \Phi_{AB} \otimes \rho_E$
Eve is completely uncorrelated with the key



Security Complications

Noise & loss in the quantum channel complicate matters

- 👉 Alice and Bob estimate the noise level as before.
- 👉 How do they extract a key?
- 👉 What if Eve attacks all signals at once? Will noise estimate work?

- ➡ When channel is noisy, they must perform **key distillation**:
 - ➡ **Information reconciliation** to correct errors
 - ➡ **Privacy amplification** to remove Eve's knowledge
- ➡ This can be seen as a form of **entanglement distillation**
 - ➡ Monogamy of entanglement again ensures privacy of key
- ➡ Randomly permuting the states takes care of coherent attacks.
 - ➡ Error-estimates still valid, even though global state is not i.i.d.
 - ➡ Suitable distillation procedures cannot tell the difference

Security Complications

Noise & loss in the quantum channel complicate matters

- ☞ Alice and Bob estimate the noise level as before.
- ☞ How do they extract a key?
- ☞ What if Eve attacks all signals at once? Will noise estimate work?

- ☞ When channel is noisy, they must perform **key distillation**:
 - ☞ **Information reconciliation** to correct errors
 - ☞ **Privacy amplification** to remove Eve's knowledge
- ☞ This can be seen as a form of **entanglement distillation**
 - ☞ Monogamy of entanglement again ensures privacy of key
- ☞ Randomly permuting the states takes care of coherent attacks.
 - ☞ Error-estimates still valid, even though global state is not i.i.d.
 - ☞ Suitable distillation procedures cannot tell the difference

Security Complications

Noise & loss in the quantum channel complicate matters

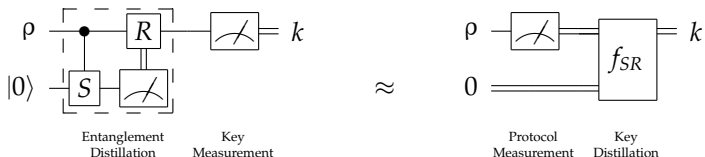
- 👉 Alice and Bob estimate the noise level as before.
- 👉 How do they extract a key?
- 👉 What if Eve attacks all signals at once? Will noise estimate work?

- ➡ When channel is noisy, they must perform **key distillation**:
 - ➡ **Information reconciliation** to correct errors
 - ➡ **Privacy amplification** to remove Eve's knowledge
- ➡ This can be seen as a form of **entanglement distillation**
 - ➡ Monogamy of entanglement again ensures privacy of key
- ➡ Randomly permuting the states takes care of coherent attacks.
 - ➡ Error-estimates still valid, even though global state is not i.i.d.
 - ➡ Suitable distillation procedures cannot tell the difference



Virtual Entanglement Distillation(?)

Wanted: Entanglement distillation scheme (S, R) such that:



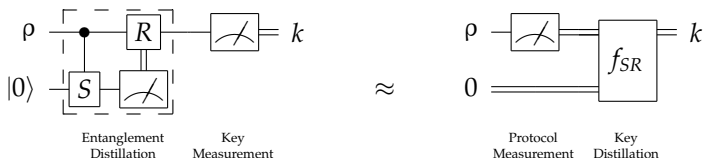
- Based on error correcting codes
- Perform bit and phase error correction separately (Like CSS codes)
 - 👉 Bit error correction \simeq information reconciliation
 - 👉 Phase error correction \simeq privacy amplification

Privacy Amplification and Phase Errors: GHZ state

- $|\psi\rangle_{ABE} = |000\rangle + |111\rangle$: Eve knows the key.
- $\rho_{AB} = \frac{1}{2} (|00\rangle + |11\rangle) = \frac{1}{2} (|\Phi^+\rangle + |\Phi^-\rangle)$: Phase error!

Virtual Entanglement Distillation(?)

Wanted: Entanglement distillation scheme (S, R) such that:



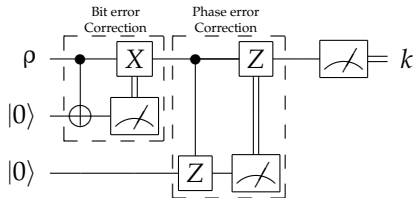
- Based on error correcting codes
- Perform bit and phase error correction separately (Like CSS codes)
 - 👉 Bit error correction \simeq information reconciliation
 - 👉 Phase error correction \simeq privacy amplification

Privacy Amplification and Phase Errors: GHZ state

- $|\psi\rangle_{ABE} = |000\rangle + |111\rangle$: Eve knows the key.
- $\rho_{AB} = \frac{1}{2} (|00\rangle + |11\rangle) = \frac{1}{2} (|\Phi^+\rangle + |\Phi^-\rangle)$: Phase error!

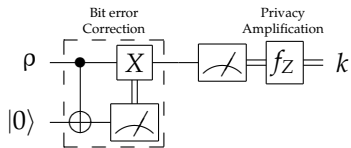


Entanglement Distillation \rightarrow Key Distillation



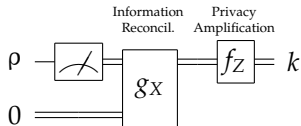
Consider latter two steps

- ☞ Project onto code subspace P
- ☞ Measure in the z basis
- ☞ Effectively measuring $P|z\rangle$



Replace with privacy amplification

- ☞ P induces an equivalence class:
 $P|z\rangle = P|z'\rangle \rightarrow z \sim z'$
- ☞ $f_Z : z \rightarrow [z]$



And finally,

Error-correction is error-correction.

Preprocessing

How can we squeeze more secret key out of raw key?

- 👉 Manipulate raw key prior to key distillation: preprocessing
- 👉 Important question practically and in principle
 - Practice: software updates to existing QKD devices
Suppose Bob is a satellite...
 - Principle: entanglement distillation \simeq key distillation?
Is prepare & measure really a limitation?

Under consideration here:

- 👉 Noise-based
- 👉 Degenerate Code-based

Helpful step: Add noise!

Careless Alice allows errors into her key. Result: rate goes up!

☞ For very high channel noise rates, the secret key rate **increases** if Alice adds noise!

Renner, Gisin, Kraus
PRA 72 012332 (2005)

☞ So does the protocol's maximum tolerable noise level.

Heuristic Explanation

- Key length $\approx I(A:B) - I(A:E)$ (for one-way key distillation)
- Adding noise damages Alice-Bob correlations, but reduces Alice-Eve correlations more

Problem: Usual entanglement-distillation proofs don't cover this case



Noise-Addled State

Alice adds i.i.d. noise at rate q

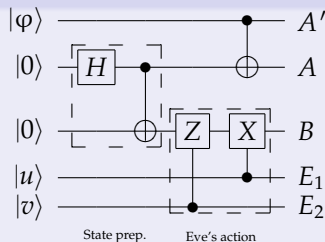
➡ noise register & control-NOT gate

👉 Start with

$$|\varphi\rangle_{A'} = \sqrt{1-q}|0\rangle + \sqrt{q}|1\rangle$$

👉 Apply CNOT $_{A' \rightarrow A}$

➡ System A' doesn't belong to Eve



$$|\psi\rangle_{ABA'E} = \sum_{\mathbf{u}, \mathbf{v}, \mathbf{f}} \sqrt{p_{\mathbf{u}, \mathbf{v}} q_{\mathbf{f}}} (X^{\mathbf{f}} \otimes X^{\mathbf{u}} Z^{\mathbf{v}}) |\Phi\rangle_{AB}^{\otimes n} |\mathbf{f}\rangle_{A'} |\mathbf{u}, \mathbf{v}\rangle_E$$

But,

👉 Entanglement distillation cares only about the key, ρ_{AB} .

👉 Assumes Eve controls everything else: $\rho_{AB} = \text{Tr}_E[\psi_{ABE}]$



Private keys come from Twisted States

- Q Keys derived from maximally-entangled states are private, but are private keys always derived from such states?
- A No. *Twisted states* are the most general states leading to private keys. Horodecki³, Oppenheim
PRL **94** 160502 (2005)

Twisted State: $\gamma_{ABA'B'}$ such that

- 1 Systems A and B are perfectly correlated & random (key)
 - 2 Eve holds purification and $\gamma_E^j = \gamma_E^k$ for all key values j, k .
- ⇒ Systems A' and B' “shield” the key from Eve

Simple form: $\gamma_{ABA'B'} = U_{\text{twist}} (\Phi_{AB} \otimes \sigma_{A'B'}) U_{\text{twist}}^\dagger$

⇒ $U_{\text{twist}} = \sum_j |jj\rangle_{AB} \langle jj| \otimes V_{A'B'}^{(j)}$

⇒ $\sigma_{A'B'}$ arbitrary

Distilling Twisted States

Lazy approach: reuse entanglement distillation methods!

Input noise-added state

$$\text{👉 } |\psi_0\rangle_{ABA'E} = \sum_{\mathbf{u}, \mathbf{v}, \mathbf{f}} \sqrt{p_{\mathbf{u}, \mathbf{v}} q_{\mathbf{f}}} (X^{\mathbf{f}} \otimes X^{\mathbf{u}} Z^{\mathbf{v}}) |\Phi\rangle_{AB}^{\otimes n} |\mathbf{f}\rangle_{A'} |\mathbf{u}, \mathbf{v}\rangle_E$$

“Offline” Bit error correction yields (Like breeding entanglement distillation protocol)

$$\text{👉 } |\psi_1\rangle_{ABA'B'E} = \sum_{\mathbf{u}, \mathbf{v}, \mathbf{f}} \sqrt{p_{\mathbf{u}, \mathbf{v}} q_{\mathbf{f}}} (\mathbb{1} \otimes Z^{\mathbf{v}}) |\Phi\rangle_{AB}^{\otimes n} Z^{\mathbf{v}} |\mathbf{f}\rangle_{A'} |\mathbf{u} + \mathbf{f}\rangle_{B'} |\mathbf{u}, \mathbf{v}\rangle_E$$

Clean up shield with CNOT from A' to B'

$$\text{👉 } |\psi_2\rangle_{ABA'B'E} = \sum_{\mathbf{u}, \mathbf{v}} \sqrt{p_{\mathbf{u}, \mathbf{v}}} (\mathbb{1} \otimes Z^{\mathbf{v}}) |\Phi\rangle_{AB}^{\otimes n} |\varphi^{\mathbf{v}}\rangle_{A'} |\mathbf{u}\rangle_{B'} |\mathbf{u}, \mathbf{v}\rangle_E$$

$$\text{👉 } |\varphi^{\mathbf{v}}\rangle = Z^{\mathbf{v}} |\varphi\rangle^{\otimes n} = \sum_{\mathbf{f}} \sqrt{q_{\mathbf{f}}} Z^{\mathbf{v}} |\mathbf{f}\rangle$$

Untwisting trick: If $|\varphi^{\mathbf{v}}\rangle$ were distinguishable...

➡ Apply controlled-Z to A and correct the phase errors

$$\text{➡ } U_{\text{twist}} = \left(\sum_{\mathbf{v}} |\varphi^{\mathbf{v}}\rangle_{A'} \langle \varphi^{\mathbf{v}}| \otimes Z_A^{\mathbf{v}} \right) \text{CNOT}_{A'B'}$$



Distinguishing the $|\varphi^{\mathbf{v}}\rangle$

Reduced state of system A' :

☞ $\rho_{A'} = \sum_{\mathbf{v}} p_{\mathbf{v}} |\varphi^{\mathbf{v}}\rangle \langle \varphi^{\mathbf{v}}|$

☞ Describes message \mathbf{v} encoded in $|\varphi^{\mathbf{v}}\rangle$ with (i.i.d.) probability $p_{\mathbf{v}}$.

Classical communication using quantum signals: HSW Theorem

☞ Any random set of $\approx 2^{nS(\sigma)}$ of the $|\varphi^{\mathbf{v}}\rangle$ are distinguishable

☞ $\sigma = (1-p)|\varphi\rangle\langle\varphi| + pZ|\varphi\rangle\langle\varphi|Z.$

☞ Use the pretty-good measurement to discriminate.

Use a random phase error correcting code to select this subset

☞ Code doesn't correct all errors, but leaves $\approx 2^{nS(\sigma)}$

☞ Untwisting operator takes care of the rest

☞ Overall key rate: $r = 1 - H(p_u) - \sum_u p_u [H(p_{v|u}) - S(\sigma_u)]$

☞ Rates for BB84 and six-state agree with RGK.



Degenerate Codes in QKD

Degeneracy: several errors have *identical action* on the code space

Example

Concatenate majority vote (for bits) and random code

- Degeneracy comes from the majority vote code
- Codewords $|\bar{0}\rangle = |00\dots 0\rangle$ and $|\bar{1}\rangle = |11\dots 1\rangle$.
- Errors Z_j all have the same effect on $|\bar{0}\rangle, |\bar{1}\rangle$

Entanglement-based picture suggests use in key distillation

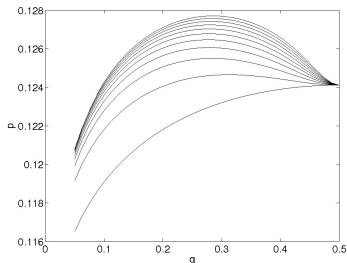
- Six-state protocol: Hoi-Kwong Lo
QIC 1 81 (2001)
- Why? Degen. codes have higher capacity than random codes...
- So, they might improve key distillation rate, too.



Degenerate Code-based Preprocessing

Changes to the protocol

- Alice adds noise at rate q
- Use length- m repetition code to correct bit errors
- Continue with the “processing”: information reconciliation and privacy amplification, based on random codes.
- Bob conditions the random code on the rep. code syndromes



BB84 Noise Threshold p

- as a function of q
- for $m = 1, m = 10, 20, \dots, 100$
- Optimal q increases with m
- $m = 400$ and $q = 0.32$:
 $p = 12.92\%$



Conclusion & Open Questions

What we now know:

- 👉 How to extend entanglement-distillation proof techniques to private-state distillation
 - 😊 Applied to noisy preprocessing: JMR and Graeme Smith, [quant-ph/0603262](#)
 - 😊 Using degenerate codes: G. Smith, JMR, and John A. Smolin, [quant-ph/0607018](#)
- 👉 Insight into the *mechanism* of key distillation

What we'd like to know:

- Other types of preprocessing? phase repetition code?
- How can phase errors be “diverted” into the shield?
- Ultimate goal: What is possible in principle?
- What is the relationship between entanglement- and key-distillation?

