

Effective Channels in Quantum Key Distribution

Joseph M. Renes

Quantum Information Theory Group (QIT)
Institut für Theoretische Physik I
Institut für Optik, Information und Photonik
Universität Erlangen-Nürnberg

2005 July 24



Two Tasks a QKD Protocol Must Perform

Any QKD protocol must perform two separate tasks:

- 1 Create a shared string:
Clearly, Alice and Bob must have a method to *decode* the quantum signals into (hopefully) identical key strings.
- 2 Estimate parameters of the quantum channel:
Knowing the details of the quantum channel, Alice and Bob can perform virtual quantum error-correction to ensure that the final key is secure.

Symmetry inherent in step #1 simplifies step #2

⇒ This creates an *effective* quantum channel whose parameters are easier to evaluate.



Two Tasks a QKD Protocol Must Perform

Any QKD protocol must perform two separate tasks:

1 Create a shared string:

Clearly, Alice and Bob must have a method to *decode* the quantum signals into (hopefully) identical key strings.

2 Estimate parameters of the quantum channel:

Knowing the details of the quantum channel, Alice and Bob can perform virtual quantum error-correction to ensure that the final key is secure.

Symmetry inherent in step #1 simplifies step #2

⇒ This creates an *effective* quantum channel whose parameters are easier to evaluate.



Two Tasks a QKD Protocol Must Perform

Any QKD protocol must perform two separate tasks:

1 Create a shared string:

Clearly, Alice and Bob must have a method to *decode* the quantum signals into (hopefully) identical key strings.

2 Estimate parameters of the quantum channel:

Knowing the details of the quantum channel, Alice and Bob can perform virtual quantum error-correction to ensure that the final key is secure.

Symmetry inherent in step #1 simplifies step #2

⇒ This creates an *effective* quantum channel whose parameters are easier to evaluate.



Two Tasks a QKD Protocol Must Perform

Any QKD protocol must perform two separate tasks:

1 Create a shared string:

Clearly, Alice and Bob must have a method to *decode* the quantum signals into (hopefully) identical key strings.

2 Estimate parameters of the quantum channel:

Knowing the details of the quantum channel, Alice and Bob can perform virtual quantum error-correction to ensure that the final key is secure.

Symmetry inherent in step #1 simplifies step #2

⇒ This creates an *effective* quantum channel whose parameters are easier to evaluate.



Decoding Quantum Signals into Classical Strings

- Generic protocol: signals $\{|\phi_j\rangle\}$ & measurement set $\{|\psi_k\rangle\}$.
Goal is to produce key letters $1, \dots, m$.
- Alice's j th decoding: $|\phi_{j_1}\rangle \rightarrow 1, |\phi_{j_2}\rangle \rightarrow 2, \dots$ etc.
Write this as $(|\phi_{j_1}\rangle, \dots, |\phi_{j_m}\rangle)$, similarly for Bob using $|\psi_{j_i}\rangle$.
Parties communicate in order coordinate decoding functions.
- BB84 protocol:
Polarizations $\{—, |, \odot, \ominus\}$ for signals & measurement.
Decoding functions (both parties):

$$(—, |), (|, —), (\odot, \ominus), (\ominus, \odot)$$

Alice announces her decoding function;
if Bob can match it, a bit is created.



Decoding Quantum Signals into Classical Strings

- Generic protocol: signals $\{|\phi_j\rangle\}$ & measurement set $\{|\psi_k\rangle\}$.
Goal is to produce key letters $1, \dots, m$.
- Alice's j th decoding: $|\phi_{j_1}\rangle \rightarrow 1, |\phi_{j_2}\rangle \rightarrow 2, \dots$ etc.
Write this as $(|\phi_{j_1}\rangle, \dots, |\phi_{j_m}\rangle)$, similarly for Bob using $|\psi_{j_i}\rangle$.
Parties communicate in order coordinate decoding functions.
- BB84 protocol:
Polarizations $\{—, |, \odot, \ominus\}$ for signals & measurement.
Decoding functions (both parties):

$$(—, |), (|, —), (\odot, \ominus), (\ominus, \odot)$$

Alice announces her decoding function;
if Bob can match it, a bit is created.



Decoding in the Quantum Version

Quantum Version of Protocol

Alice starts with $|\Phi\rangle = \sum_k |k\rangle_A |\phi_k\rangle_B$, sends half to Bob.

Bob makes Neumark extension: $|\Phi'\rangle = \sum_{k\ell} |k\rangle_A |\ell\rangle_B \langle\psi_\ell|\phi_k\rangle$.

- Standard basis mmt. completes quantum phase of protocol; Then comes decoding and further classical postprocessing.
- Interchange the order and perform decoding *first*. This yields an entangled state, which then gives the key.

Decoding function \Rightarrow projection operator $\Pi_i = \sum_k |k\rangle\langle i_k|$.

Decoded state $\Rightarrow |\Phi_{ij}\rangle = \sum_{k\ell} |k\rangle_A |\ell\rangle_B \langle\psi_j|\phi_{i_k}\rangle$



Decoding in the Quantum Version

Quantum Version of Protocol

Alice starts with $|\Phi\rangle = \sum_k |k\rangle_A |\phi_k\rangle_B$, sends half to Bob.

Bob makes Neumark extension: $|\Phi'\rangle = \sum_{k\ell} |k\rangle_A |\ell\rangle_B \langle\psi_\ell|\phi_k\rangle$.

- Standard basis mmt. completes quantum phase of protocol; Then comes decoding and further classical postprocessing.
- Interchange the order and perform decoding *first*. This yields an entangled state, which then gives the key.

Decoding function \Rightarrow projection operator $\Pi_i = \sum_k |k\rangle\langle i_k|$.

Decoded state $\Rightarrow |\Phi_{ij}\rangle = \sum_{k\ell} |k\rangle_A |\ell\rangle_B \langle\psi_j|\phi_{i_k}\rangle$



Symmetries of the decoded state

- Now forget decoding info. Final state becomes the mixture:

$$\rho = \sum_{ij} |\Phi_{ij}\rangle\langle\Phi_{ij}|.$$

- ρ invariant under unitaries U_π and V_π which permute the decoding functions: $U_\pi|\phi_{i_k}\rangle = |\phi_{\pi(i)_k}\rangle$, $V_\pi|\psi_{j_\ell}\rangle = |\psi_{\pi(j)_\ell}\rangle$

Key letter stays the same, but it comes from a different signal/mmt state.

- Quantum channel is described by $\mathcal{E}(\rho) = \sum_p E_p \rho E_p^\dagger$.
- Decoding symmetry reduces this to

$$\mathcal{E}_{\text{sym}}(\rho) = \sum_{\rho, \pi} V_\pi^\dagger E_p U_\pi \rho U_\pi^\dagger E_p^\dagger V_\pi.$$

- Effective channel \mathcal{E}_{sym} invariant under decoding symmetry.



Symmetries of the decoded state

- Now forget decoding info. Final state becomes the mixture:

$$\rho = \sum_{ij} |\Phi_{ij}\rangle\langle\Phi_{ij}|.$$

- ρ invariant under unitaries U_π and V_π which permute the decoding functions: $U_\pi|\phi_{i_k}\rangle = |\phi_{\pi(i)_k}\rangle$, $V_\pi|\psi_{j_\ell}\rangle = |\psi_{\pi(j)_\ell}\rangle$

Key letter stays the same, but it comes from a different signal/mmt state.

- Quantum channel is described by $\mathcal{E}(\rho) = \sum_p E_p \rho E_p^\dagger$.
- Decoding symmetry reduces this to

$$\mathcal{E}_{\text{sym}}(\rho) = \sum_{\rho, \pi} V_\pi^\dagger E_p U_\pi \rho U_\pi^\dagger E_p^\dagger V_\pi.$$

- Effective channel \mathcal{E}_{sym} invariant under decoding symmetry.



Conclusion

Decoding symmetry creates an effective quantum channel \mathcal{E}_{sym} .

- Easier to estimate parameters of \mathcal{E}_{sym} than \mathcal{E}
 - Use channel estimate in Shor-Preskill virtual quantum error-correction security proof.
 - Details in J. M. Renes and M. Grassl, *Generalized decoding, effective channels, and simplified security proofs in quantum key distribution*, [quant-ph/0505061](https://arxiv.org/abs/quant-ph/0505061).
- ⇒ Tetrahedron protocol of PRA **70**, 052314 (2004) secure to 11.56% error.
- ⇒ Qutrit spherical code protocols of QIC **5**, 080-091 (2005) also tabulated.

