SECURITY, FINITE KEY, AND QUANTUM REPEATERS

Silvestre Abruzzo, Sylvia Bratzik, Markus Mertz, Hermann Kampermann, and Dagmar Bruß

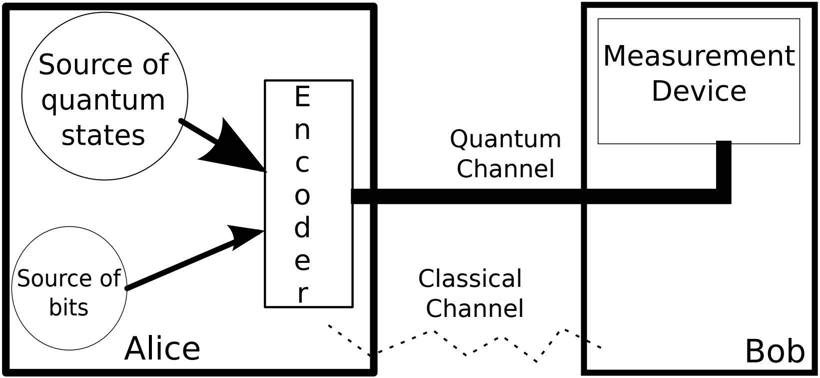
Heinrich-Heine-Universität Düsseldorf

Institut für Theoretische Physik III

GEFÖRDERT VOM

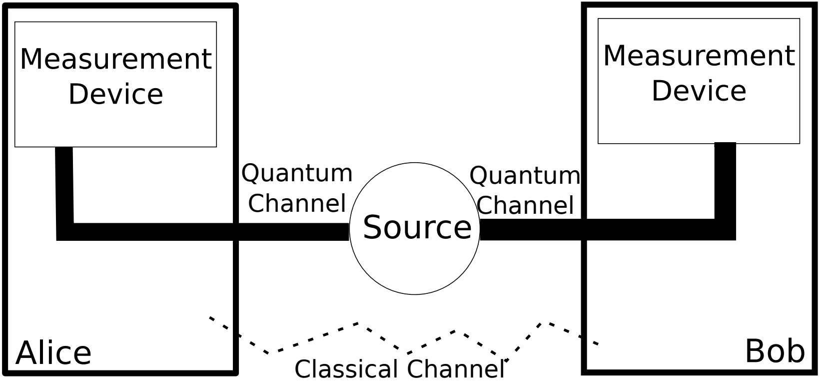
Bundesministerium für Bildung und Forschung

QKD prepare and measure



1. Alice encodes classical values in quantum states.
2. Quantum states are sent through the quantum channel.
3. Bob decodes quantum states in order to obtain classical values.

Entanglement-based QKD



1. Source produces entangled qubits.
2. Alice and Bob perform measurements.

When devices are perfect

Prepare and measure $\equiv$ Entanglement-based

$\Rightarrow$ Security of one implies security of the other one.

A simply proof is in T. Meyer, PhD Thesis,

http://docserv.uni-duesseldorf.de/servlets/DerivateServlet/Derivate-6444/thesis_noextras.pdf

QKD protocol

1. Creation and distribution: N_{SOURCE} pulses are produced.
2. Measurement: A & B choose at random and independently the measurement basis and measure
3. Sifting: discard measurements where Alice and Bob used a different basis.

Classical post-processing

1. Parameter estimation(PE):
   - estimated Quantum Bit Error Rate (QBER) e.
   - If e too big the protocol is aborted.
2. Error correction(EC): Alice sends an error correction code to Bob.
3. Error verification(EV): it is verified that the EC protocol worked.
4. Privacy amplification(PA): the corrected string is shrunk and a final key of length ℓ is obtained.

NEXT STEP: Provide a connection between ℓ and N_{source}.

Same definitions

- Shannon entropy: $H(X)_P := -\sum_{x\in\mathcal{X}} P_X(x)\log_2 P_X(x)$.
- Von Neumann entropy: $S(X)_\rho := -tr(\rho \log_2 \rho)$.
- Mutual information:
  $I(X;Y)_P := H(X)_P + H(Y)_P - H(X,Y)_P$.
- Classical Conditional entropy:
  $H(X|Y)_P := H(X;Y)_P - H(Y)_P$
- Quantum Conditional entropy:
  $S(X|Y)_\rho := S(X;Y)_\rho - S(Y)_\rho$.
- Binary entropy: $h(p) := -p\log_2 p - (1-p)\log_2(1-p)$.

Definition of security

Classical security

- X random variable describing the possible keys
- E random variable describing Eve's information

A key (of length ℓ) is ε-secure if

$$H(X) \geq \ell - \varepsilon \qquad (1)$$

$$I(X;E) \leq \varepsilon \qquad (2)$$

Ahlswede, R.; Csiszar, I.; IEEE 39 Issue:4, 1993.

Quantum security

- X random variable describing the possible keys
- $\mathcal{M}(\rho_E)$ random variable obtained when E applies POVM $\mathcal{M}$ on ρ_E

A key (of length ℓ) **was** ε-secure if

$$H(X) \geq \ell - \varepsilon \qquad (3)$$

$$\max_{\mathcal{M}} I(X;\mathcal{M}(\rho_E)) \leq \varepsilon \qquad (4)$$

H.-K. Lo and H. F. Chau, Science 283, 2050 (1999).

The quantum definition is problematic:

(Robert König, Renato Renner, et *al.* Phys. Rev. Lett. 98, 140502 (2007))

1. Not composable.
2. No operational meaning for ε.

Trace distance definition of security

$\rho_{K^\ell E^\ell}$ key + Eve's quantum state

ε-security

A key K^ℓ is ε-secure if [a]

$$\min_{\tau_E} \frac{1}{2} \left\| \rho_{K^\ell E^\ell} - \frac{1}{2^\ell} \mathbb{1} \otimes \tau_E \right\|_1 \leq \varepsilon,$$

where $\|A\|_1 := \mathrm{tr}(\sqrt{AA^\dagger})$ and $0 \leq \varepsilon \leq 1$ is the security parameter.

[a] Renner, R., International Journal of Quantum Information (IJQI), ETH Zurich, 2008

Properties:

1. Composable.
2. Meaning for ε.

Eve's attacks

$\rho_{A^{N_\text{source}}B^{N_\text{source}}}$: Alice and Bob system

1. Collective attacks: final state tensor product
   $\rho_{A^{N_\text{source}}B^{N_\text{source}}} = \rho_{AB}^{\otimes N_\text{source}}$
2. Coherent attacks: no assumption on $\rho_{A^{N_\text{source}}B^{N_\text{source}}}$

For an arbitrary long key, ensuring particular symmetries

Coherent attacks$\equiv$collective attacks

Kraus, Gisin, Renner, Phys. Rev. Lett. 95, 080501 (2005)

What is the best state for the eavesdropper?

Definition

The state $|\psi\rangle_{ABE}$ is a purification of ρ_{AB} iff $\rho_{AB} = \mathrm{tr}_E\left(|\psi\rangle_{ABE}\langle\psi|\right)$.

$\Rightarrow$The BEST FOR THE EAVESDROPPER: obtain

$$\rho_E = \mathrm{tr}_{AB}\left(|\psi\rangle_{ABE}\langle\psi|\right).$$

Rev. Mod. Phys. 81, 1301–1350 (2009)

Formula for the asymptotic secret key rate

I. Devetak and A. Winter, Proc. R. Soc. Lond. A 461, 207 (2005)

n:=number of bits remained after PE

$\rho_{X^nY^nE^n} = \rho_{XYE}^{\otimes n}$ state describing Alice's string (X) + Bob's string (Y) + Eve's system (E)

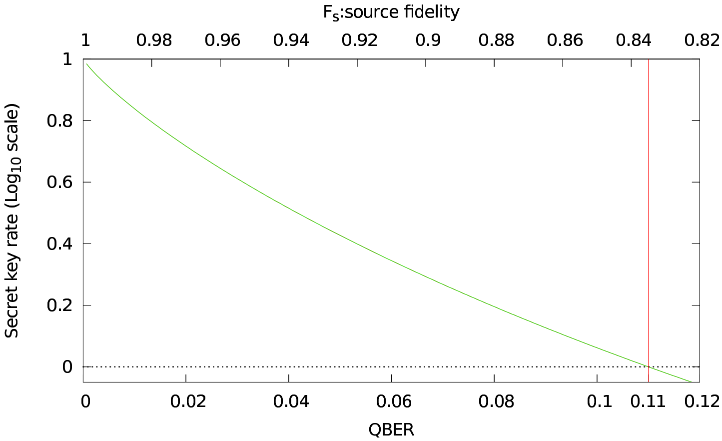
$$r_\infty := \underbrace{S(X|E)_\rho}_{PA} - \underbrace{H(X|Y)_\rho}_{EC}.$$

Two examples:

Rev. Mod. Phys. 81, 1301–1350 (2009)

- BB84: $1 - h(e_X) - h(e_Y)$
- six-state protocol: $1 - e_Z h\left(\frac{1+(e_X-e_Y)/e_Z}{2}\right) - (1-e_Z)h\left(\frac{1-(e_X+e_Y+e_Z)/2}{1-e_Z}\right) - h(e_Z)$

BB84 (isotropic channel)



Secret key length

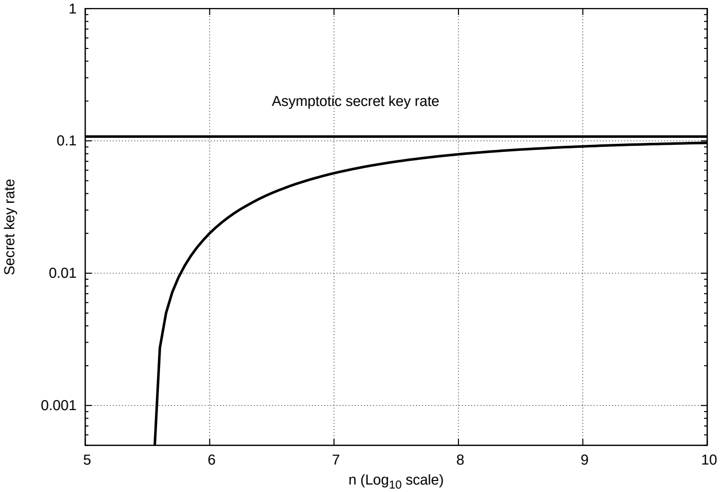
Using the framework of the finite-key analysis the following result holds.

Theorem: If Alice and Bob distill a secret key of length

$$\ell \leq \max_{\substack{\bar{\varepsilon}, \varepsilon_{\rm PE}, \varepsilon_{\rm PA} \\ 0 \leq \bar{\varepsilon} + \varepsilon_{\rm EC} + \varepsilon_{\rm PA} + \varepsilon_{\rm PE} \leq \varepsilon}} \left[n \left(\underbrace{S(X|E)_\rho}_{PA} - \underbrace{5\sqrt{\log_2\left(\frac{2}{\bar{\varepsilon}}\right)\frac{1}{n}}}_{\text{Finite correction}} - \underbrace{f_{\rm EC} H(X|Y)_\rho}_{EC} \right) - \underbrace{\log_2 \frac{2}{\varepsilon_{\rm EC}}}_{EV} - \underbrace{2\log_2 \frac{1}{\varepsilon_{\rm PA}}}_{\varepsilon\text{-security}} \right],$$

then it is ε-secure.

Finite-key analysis



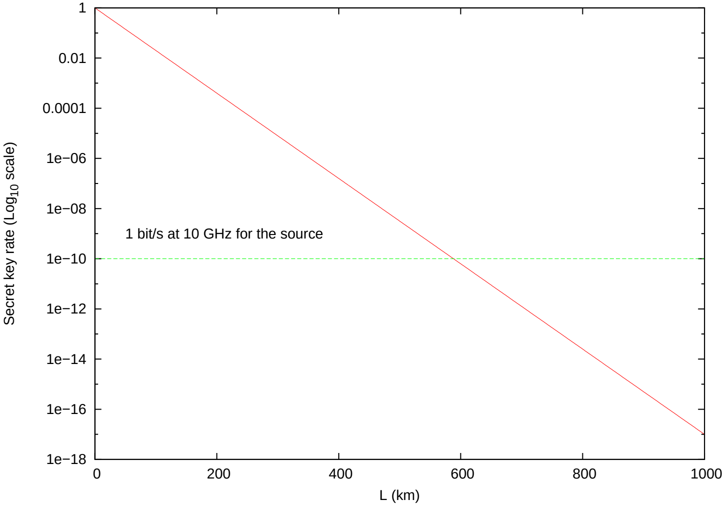
Imperfections

- Detectors: η_D: efficiency, p_{DARK}: dark count probability
- Quantum channel: losses and decoherence
- Source: no single-photon source, no bell states source

Rev. Mod. Phys. 81, 1301–1350 (2009)

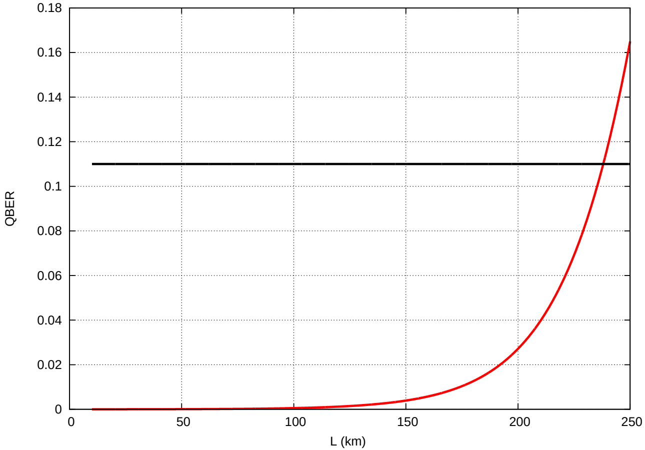
Effect of losses

Perfect detectors, perfect source, no decoherence; Optical fiber $t_{link}(L) = 10^{-\frac{\alpha L}{10}}$ with $\alpha = 0.17 dB/Km$.



Effect of imperfect detectors

$$QBER = QBER_{\text{Channel}} + QBER_{\text{DarkCounts}}$$



BB84, $\eta_D = 0.95$, $p_{\text{Dark}} = 10^{-5}$

Effect of imperfect source

Ideal state

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|11\rangle + |00\rangle)$$

Real produced state

$$\rho = F|\psi^+\rangle\langle\psi^+| + \left(\frac{1-F}{3}\right)(|\psi^-\rangle\langle\psi^-| + |\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-|)$$

Other possible imperfections:

- multi-photon pulses
- pulses produced probabilistically

How to calculate the secret key rate

1. create a model of the set-up and all imperfections
2. calculate the raw key rate $R_{\text{raw}} = \frac{\text{Number of measurements}}{\text{Number of initial pulses}}$
3. calculate the QBER e
4. calculate the secret fraction $r(e) = \frac{\text{Number of secure bits}}{\text{Number of measurements}}$
5. the total rate is $K = R_{\text{raw}} r(e)$

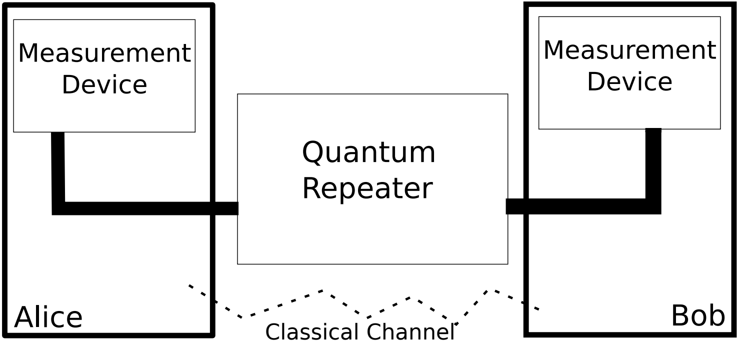
Introduction

Entanglement swapping: 2 short-distance entangled pairs $\Rightarrow$ 1 long-distance entangled pair
Distillation: N pairs with fidelity $F_0 \Rightarrow M < N$ pairs with fidelity $F_1 > F_0$

- Quantum relay: only entanglement swapping
  - with memory
  - without quantum memory

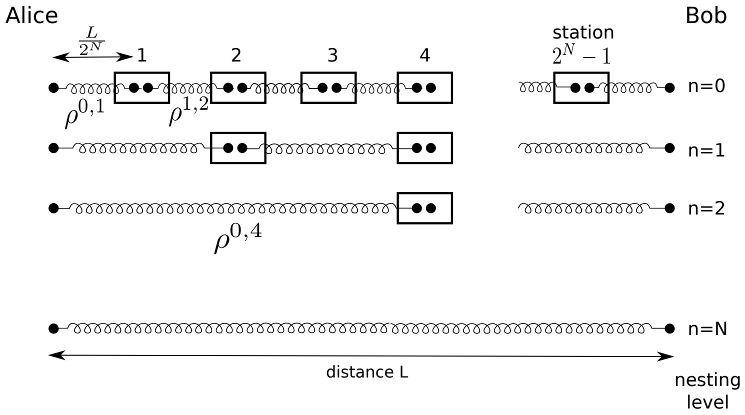
- Quantum repeater: entanglement swapping + distillation

Global scheme

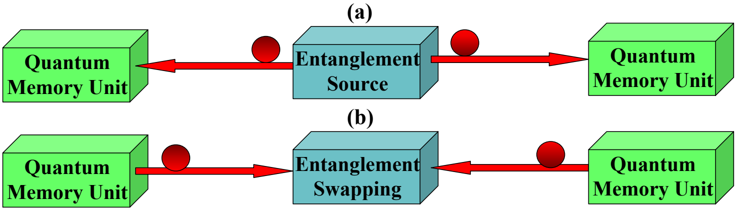


Security proof: repeater under the control of the eavesdropper

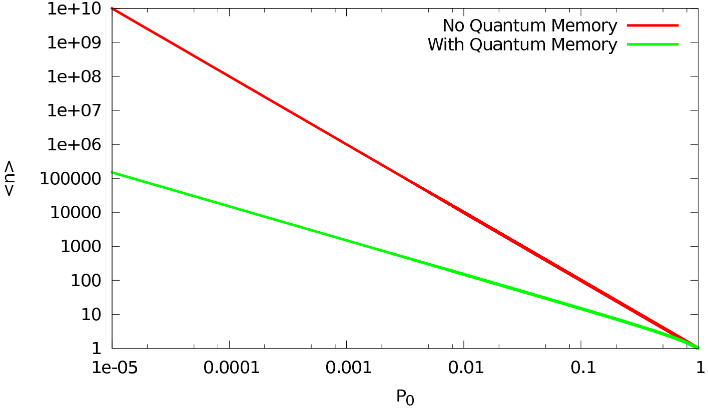
A model of quantum repeaters



How entanglement is created



On the role of quantum memories

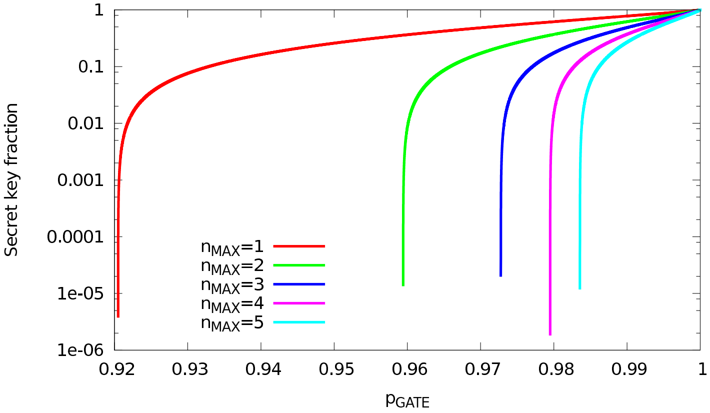


what we are doing

1. consider different model of quantum relay and calculate the secret key rate
2. consider different distillation protocols and see which one is better
3. general model for the imperfection in the gates

A specific example:Briegel-type quantum relay

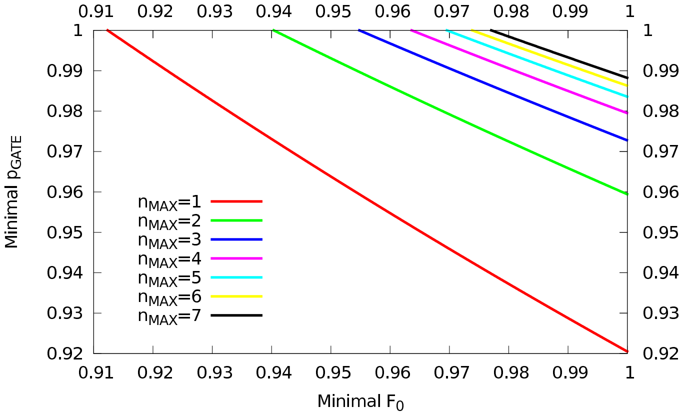
Effect of gates imperfection



BB84: perfect detectors, perfect source, perfect channel

Gates imperfection + imperfect source

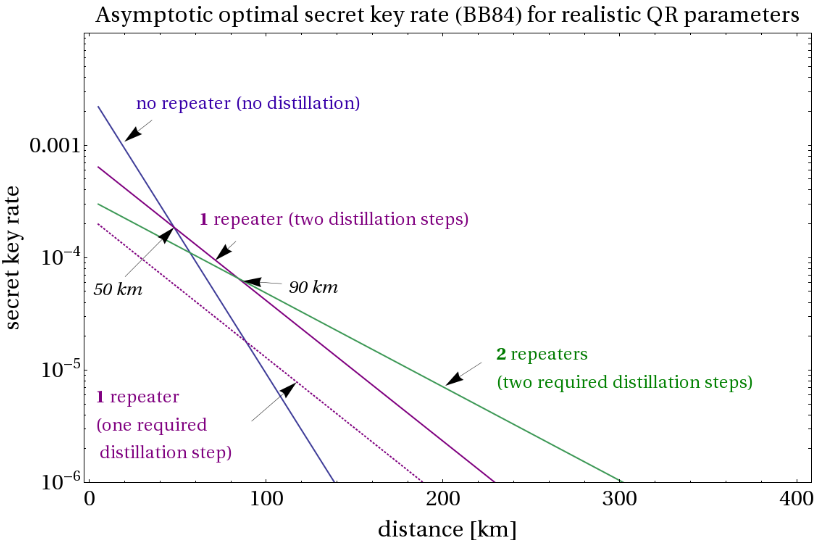
Minimal fidelity and p_{GATE} permitting to extract a key.



On-going work

- analysis other quantum repeaters architectures(Rydberg gates, Hybrid, ...)
- analysis DLCZ-type protocol

Analysis of distillation protocols



General model for imperfection

Many models of imperfections are present in literature:

1. Briegel-model, i.e. depolarization
2. diamond norm
3. gate fidelity

$\Rightarrow$ study these models in general and calculate key rates.

Conclusions

Quantum key distribution:

- Protocol: entanglement-based $\equiv$ prepare and measure
- Security: trace-distance definition, purification for the eavesdropper
- key-rate: asymptotic vs finite-size corrections
- imperfections: essential for a correct analysis

Quantum repeaters:

- General scheme
- Our work
  - Quantum relays
  - analysis of different distillation protocols
  - models for imperfections of the gates