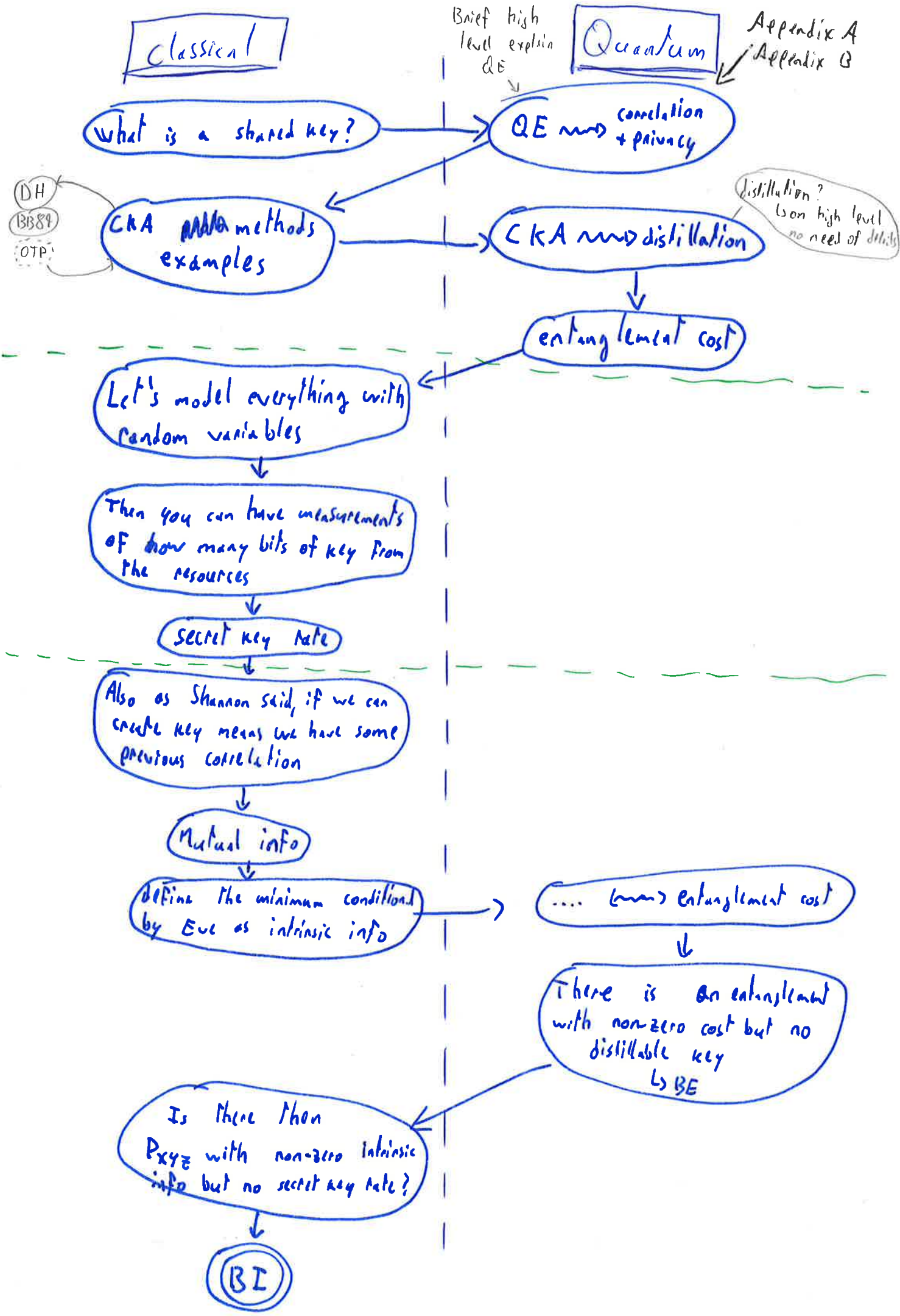
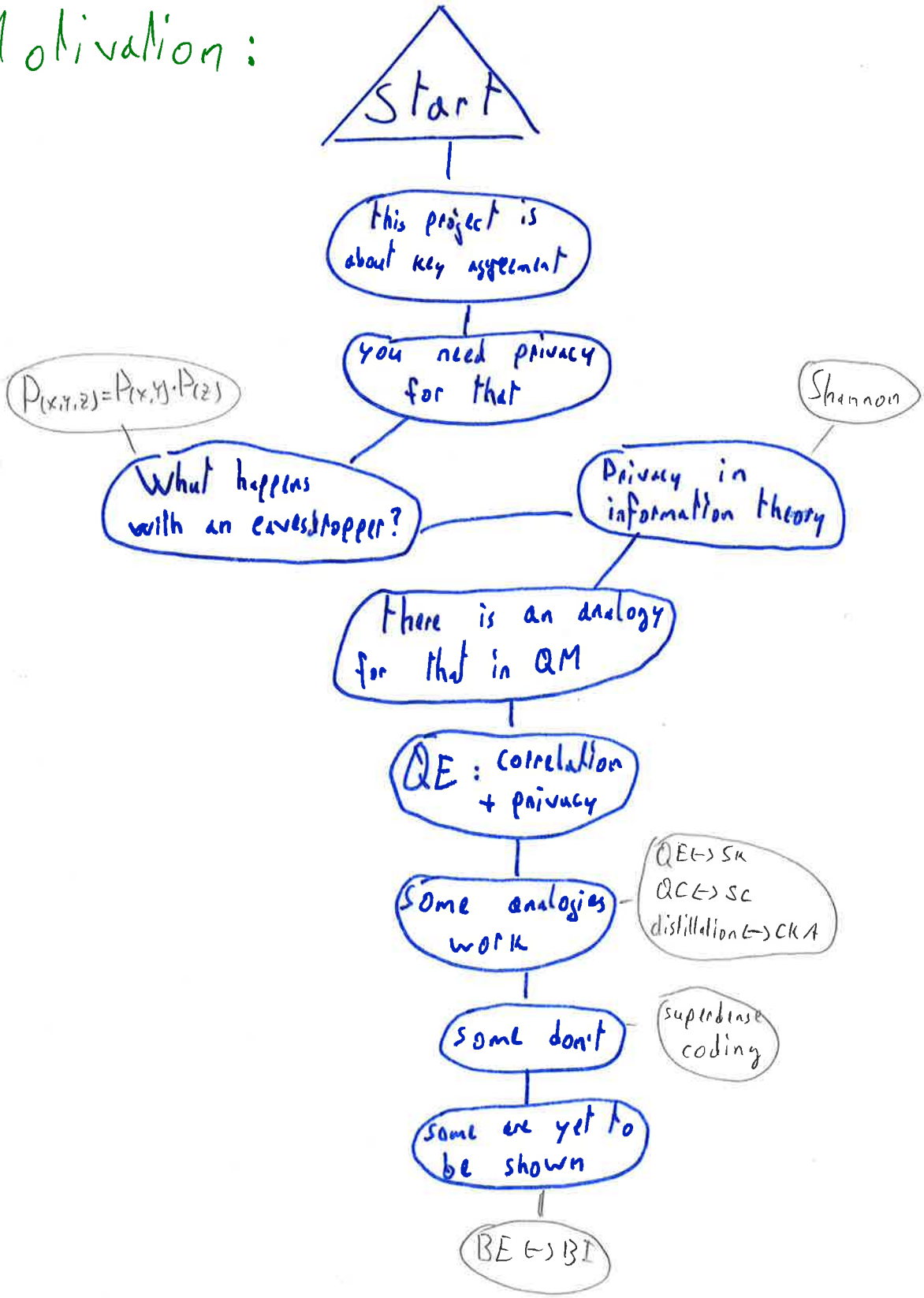
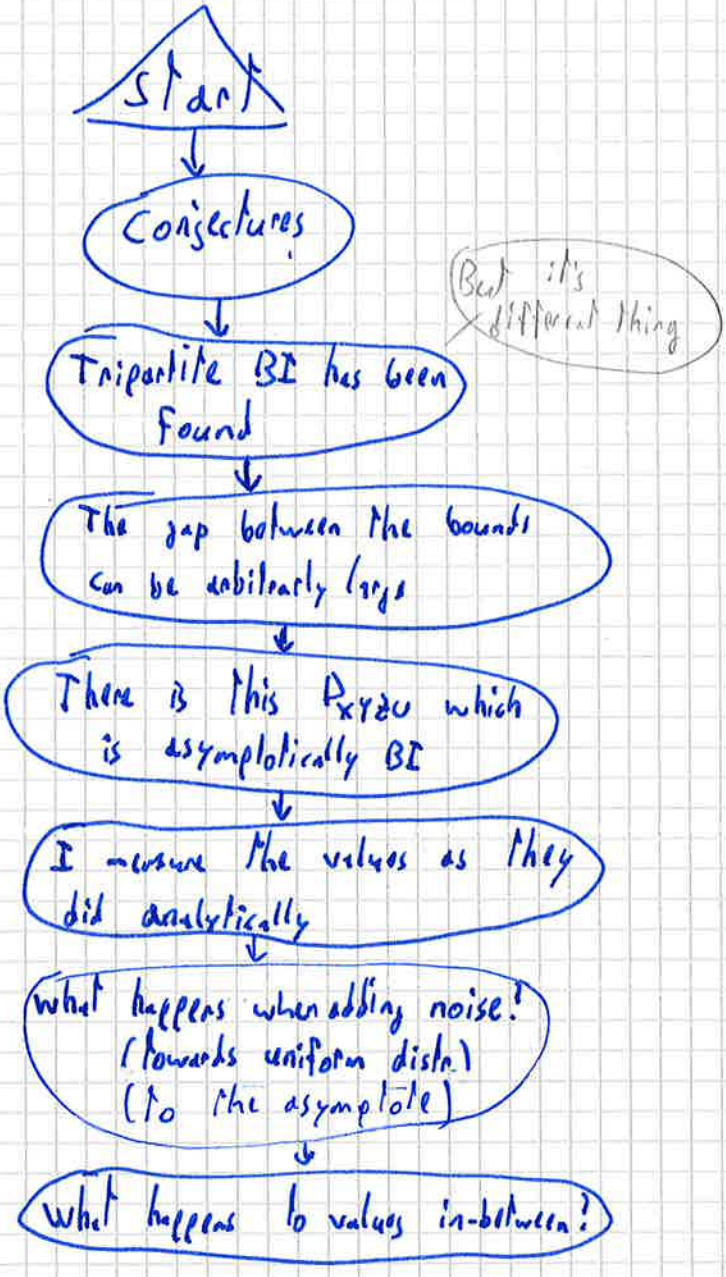

Classical
Brief high level explain QE
Quantum
Appendix A
Appendix B
What is a shared key?
QE ⇝ correlation + privacy
DH
BB84
OTP
CKA methods examples
CKA ⇝ distillation
distillation? ↳ on high level no need of details
entanglement cost
Let's model everything with random variables
Then you can have measurements of how many bits of key from the resources
secret key rate
Also as Shannon said, if we can create key means we have some previous correlation
Mutual info
define the minimum conditional by Eve as intrinsic info
.... ⇝ entanglement cost
There is an entanglement with non-zero cost but no distillable key
↳ BE
Is there then P_{XYZ} with non-zero intrinsic info but no secret key rate?
BI

Motivation:


Start
this project is about key agreement
you need privacy for that
$P_{(X,Y,Z)}=P_{(X,Y)}\cdot P_{(Z)}$
Shannon
What happens with an eavesdropper?
Privacy in information theory
There is an analogy for that in QM
QE : correlation + privacy
QE ↔ SR
QC ↔ SC
distillation ↔ CKA
some analogies work
some don't
superdense coding
some are yet to be shown
BE ↔ BI

Chapter 3



Appendix A:
Mathematical framework for QM
- Dirac
- Lin. Op. (adjoints)
- Inner prod.
- Tensor prod.

Appendix B: QM
- measurements
- entanglement

Appendix C: Inf. Theo.
- Entropy
- Channels