Discrete Variable QKD protocols
Lecture 1: Principles

Norbert Lütkenhaus

Institute for Quantum Computing, University of Waterloo

1

Secret key for secret communication

One time pad (Vernam cipher)
Alice and Bob share secret key

Alice: 0 1 0 0 1 0 1 message
XOR 1 1 0 1 0 1 0 key

1 0 0 1 1 1 1 cryptogram (public)

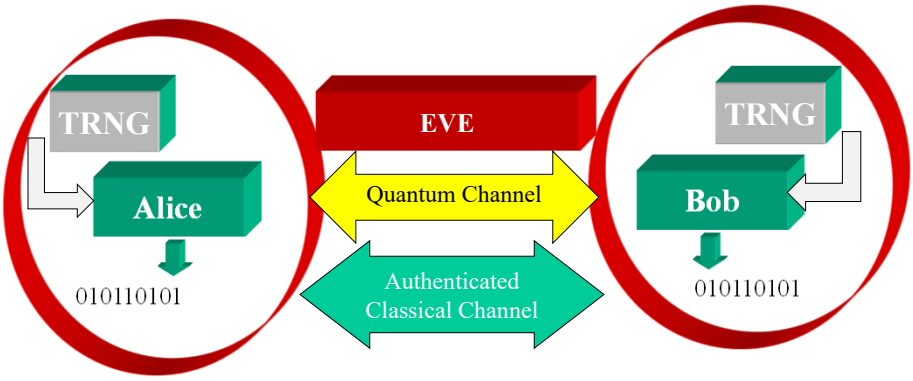
XOR 1 1 0 1 0 1 0 key
Bob: 0 1 0 0 1 0 1 message

Required key properties:
- All keys equally likely
- Key shared between Alice and Bob
- Eve knows nothing about the key

Applications of pairwise shared secret key:
- Encryption (one-time pad, seed of AES etc)
- Authentication
- Secure multi-party computations

2

Quantum Key Distribution Primitive



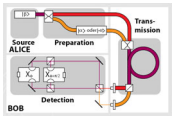
- Task: create simultaneously secret key in two distant locations
- Tool: quantum devices that we trust to do the right thing …
- Assumption: secure perimeter for Alice and Bob
- Tool: authenticated classical channel & Quantum Channel
- Tool: use of (local) true random number generators (TRNG)

3

Protocol vs Implementation security

Actual Device
e.g. reality based

modelling



Quantum Optical Model
e.g. mode based

$||\rho_{ABE} - \rho_{AB} \otimes \rho_C||_1 \leq \epsilon$

Security Proof

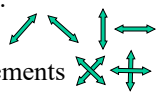
Protocol Security
(rigorous math …)

Implementation Security
(best practice …)

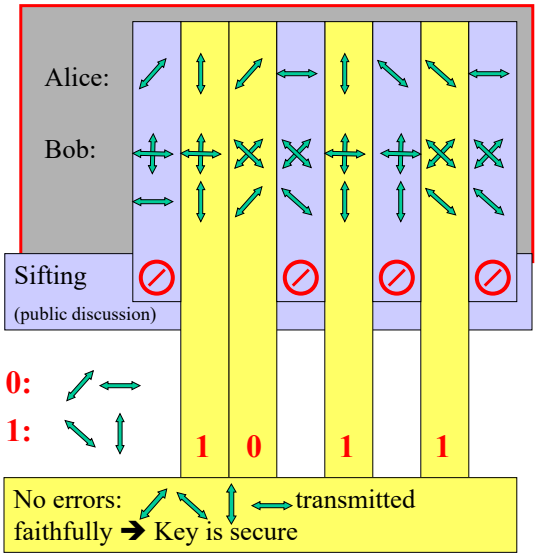
4

Bennett Brassard Protocol (1984)

Quantum Part:
Create random key:
➔random signals
➔random measurements

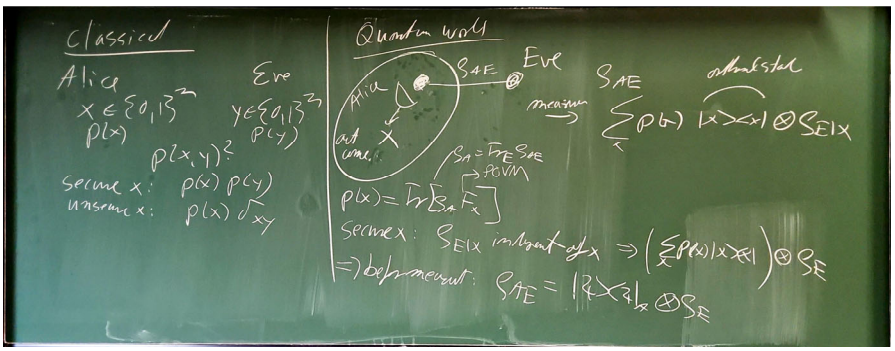


Public discussion over faithful classical channel: distinguish **deterministic** from **random processes**



5

How can Quantum Mechanics help to deliver secure key?

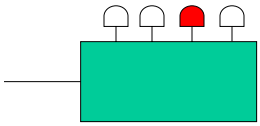


In quantum mechanics, we can under the right circumstances prove from local actions that no third parties have knowledge about classical data.

This works if the data are results from measurements on a quantum system, for which we can successfully prove that that quantum system was in a pure state.

6

Quantum Mechanics Background



Measurement:
- set of mutually exclusive outcomes
- outcome k ↔ operator F_k
- Probability rule $\Pr(k) = \langle\Psi|F_k|\Psi\rangle$

density matrix ρ

$$\rho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$$
$$\rho = \rho^\dagger$$
$$\rho \geq 0$$
$$Tr[\rho] = 1$$

Positive Operator Valued Measure (POVM) $\{F_k\}_k$

$$F_k = F_k^\dagger$$
$$F_k \geq 0$$
$$\sum_k F_k = \mathbb{1}$$

Purification of density matrix

$$\rho_A = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$$
$$|\Psi\rangle_{AE} = \sum_i \sqrt{p_i} |\Psi_i\rangle_A |i\rangle_E$$

orthonormal set $\{|i\rangle_E\}_i$

Schmidt decomposition

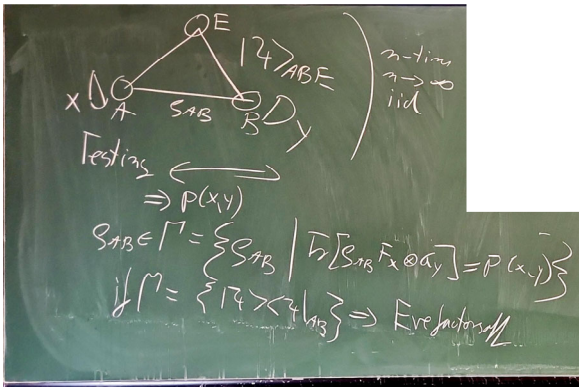
any bipartite pure state can be written as

$$|\Psi\rangle_{AE} = \sum_i \lambda_i |i\rangle_A |i\rangle_E \qquad \lambda_i > 0$$

orthonormal sets $\{|i\rangle_A\}_i$ $\{|i\rangle_E\}_i$

7

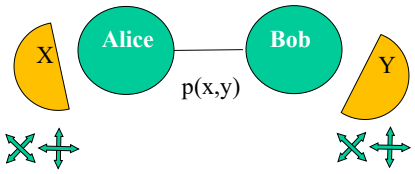
Generic Setup for Entanglement based QKD



Applied to entanglement based QKD, in some situations Alice and Bob can prove from their separable, joint measurements that only a shared pure state can explain the measurement results. That implies that Eve factors off and knows nothing about the measurement results

8

2 MUB measurements



assume observations:

P(x,y)	↕	↔	↘	↗
↕	1/8	0	1/16	1/16
↔	0	1/8	1/16	1/16
↘	1/16	1/16	1/8	0
↗	1/16	1/16	0	1/8

measurements not tomographically complete!

But ρ_{AB} must be mixture of pure states all of which are orthogonal to

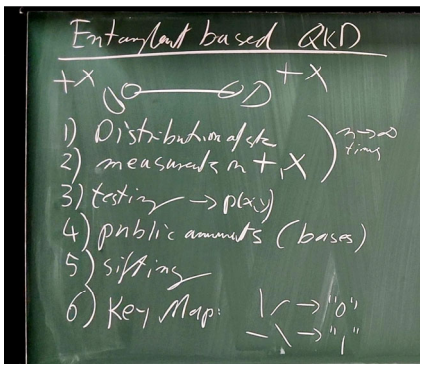
$|\updownarrow, \leftrightarrow\rangle$, $|\leftrightarrow, \updownarrow\rangle$, $|\searrow, \nearrow\rangle$, $|\nearrow, \searrow\rangle$

$$|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow,\updownarrow\rangle_{AB} + |\leftrightarrow,\leftrightarrow\rangle_{AB}\right)$$

pure state: Eve factors off➔ no correlation between Alice/Bob and Eve!

9

BBM QKD protocol

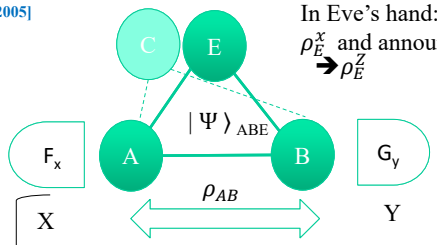


This is how we can use the observation in the previous slide to turn this into a full QKD protocol.

10

Generic QKD

[Renner, PhD Thesis 2005]



In Eve's hand:
ρ_E^x and announcement C
$\rightarrow \rho_E^Z$

Key map:
{X, C} $\rightarrow$ Z

frequency in tested signals: p(x,y)
$\rho \in \Gamma = \{\rho_{AB} \; | Tr[F_x \otimes G_y \; \rho_{AB}] = p(x,y)\}$

announcements C

Idealized Protocol Structure:
1. Distribute signals
2. Measure signals
3. Testing
4. Public announcement
5. sifting
6. Key map

Security:
- Testing reveals that Eve decouples (ideally)
- Still need to check that announcements C do not leak information!

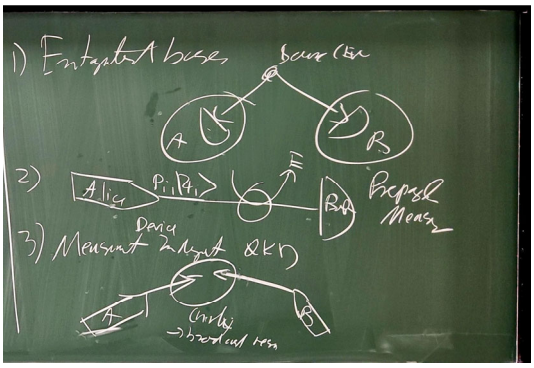
11

Schemes

1) Entanglement based QKD

2) Prepare and Measure QKD

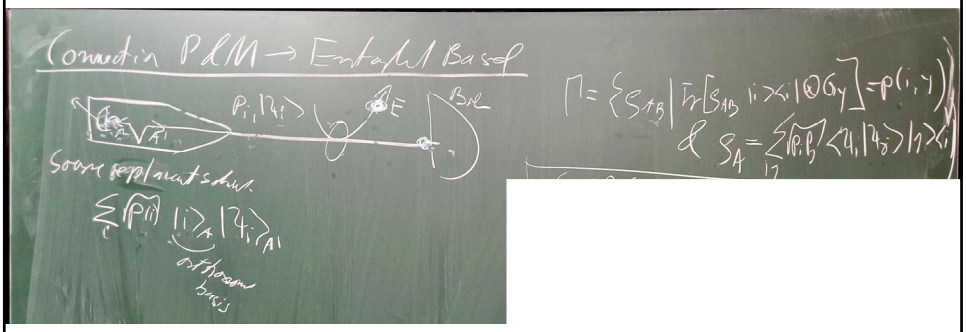
3) Measurement-Device Independent QKD



- All three schemes need trusted (characterized) devices in Alice and Bob's hand.
- MDI QKD needs also an (untrusted) third party in the middle (Charlie) that performs Bell-state measurements and announces the result.
- Only the Entanglement-based scheme with active choices of measurements is known to be also successful as Device Independent QKD without characterized Devices

12

Source Replacement Scheme

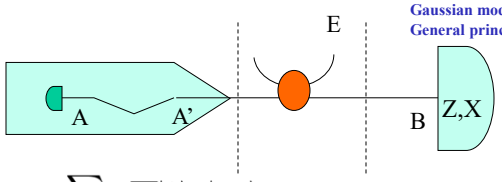


- A Source replacement scheme allows to reduce a prepare and measure setup to an entanglement based scheme.
- Only difference: in the set Gamma, we have also listed the knowledge of the marginal density matrix \rho_A, which cannot be changed by Eve. Without that constraint, we would never be able to show that Gamma contains only a pure state, as Alice measures in a von Neumann measurement …

13

Source Replacement Scheme

BB84 states: Bennett/Brassard/Mermin
Gaussian modulated CV QKD: Grosshans/Grangier
General principle: Curty/Lewenstein/NL



$$|\Psi\rangle_{A,A'} = \sum_k \sqrt{p_k}|k\rangle_A|\Psi_k\rangle_{A'}$$

$$\rho_A = \sum_{k,j} \sqrt{p_k p_j}\langle\Psi_k|\Psi_j\rangle\ |j\rangle\langle k|$$

14

Theorem

Generalized Beam-Splitting Theorem (Heid, NL)

A channel that transforms non-orthogonal pure input states $|\Psi_i\rangle_{A'}$ into pure output states $|\phi_i\rangle_B$ gives rise in to a state in the purification and source replacement view as

$$|\Psi\rangle_{ABE} = \sum_i \sqrt{p_i}|i\rangle_A|\phi_i\rangle_B|\tilde{\phi}_i\rangle_E$$

where Eve's state satisfies the overlap properties

$$\langle\Psi_i|\Psi_j\rangle_{A'} = \langle\phi_i|\phi_j\rangle_B \langle\tilde{\phi}_i|\tilde{\phi}_j\rangle_E$$

Corollary:

If the channel transmits the signals unchanged, then we have

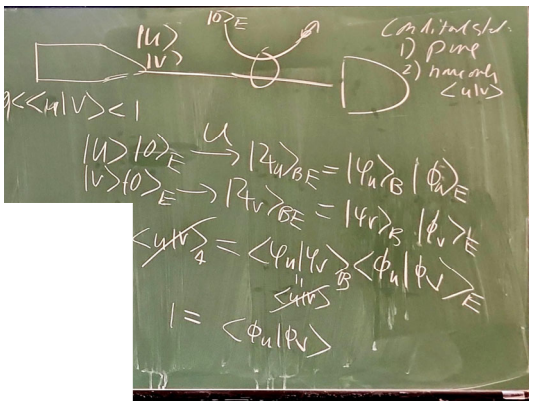
$$\langle\tilde{\phi}_i|\tilde{\phi}_j\rangle_E = 1 \quad \forall i,j$$

and Eve decouples

$$|\Psi\rangle_{ABE} = \left(\sum_i \sqrt{p_i}|i\rangle_A|\phi_i\rangle_B\right)|\tilde{\phi}\rangle_E$$

15

Proof sketch



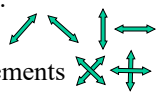
We demand that the outgoing BE state contains a pure state for Bob, so that state must factor

We additionally assume that the overlap of the pure states arriving at Bob is the same as the signal states. We then find that Eve's states are identical, meaning that Eve factors off and is not correlated with the signals.

16

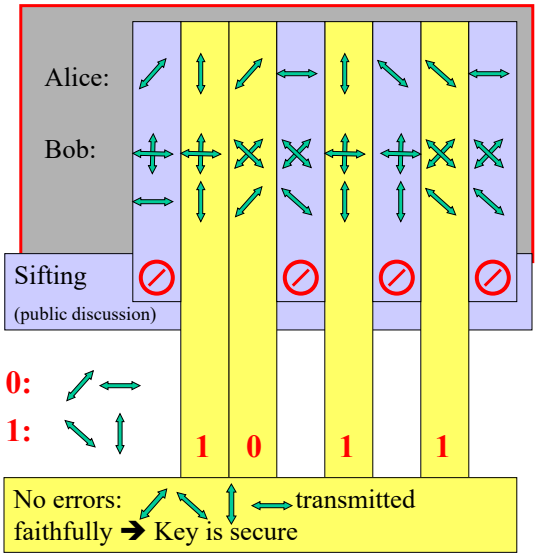
Bennett Brassard Protocol (1984)

Quantum Part:
Create random key:
➔random signals
➔random measurements



Public discussion over faithful classical channel: distinguish **deterministic** from **random processes**

No errors
➔ the four non-orthogonal signals are transmitted faithfully over the channel
➔ Eve is not correlated with Alice/Bob's data!!



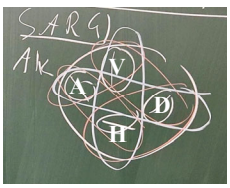
17

BB84 variations

No announcement BB84:
- do not announce the bases

➔ Testing still shows that Eve decouples
➔ However, Alice and Bob are not perfectly correlated
  ➔ Use Error correction ➔ leaks some information to Eve
  ➔ Use privacy amplification to cut out that information

SARG protocol:
- Announce not the basis, but a set of two states: the actual signal state and (at random) one of either 'neighbouring' state
- Requires post-selection (like in the B92 protocol, see next lecture) to complete the protocol



Announcement groups of H, V, A, D signals
- BB84 in white
- SARG in red

18

BB84 variations

SARG protocol [V. Scarani, A. Acin, G. Ribordy, and N. Gisin. PRL 92, 057901 (2004)]
No Public Announcement BB84 (NPAB) [Z. Wang, A. Corrigan, NL, arXiv:2603.22448]

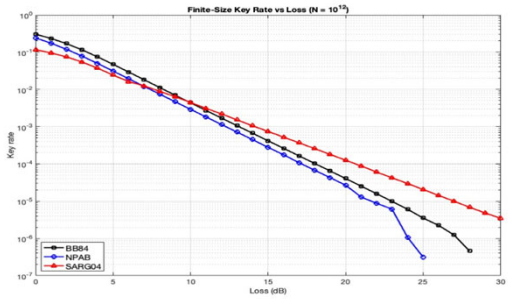


FIG. 8. Secret key rate per signal for a loss-only quantum channel for protocols with $N = 10^{12}$ total signals sent. The signal intensity is optimized.

[weak coherent pulses, no decoy states]

19

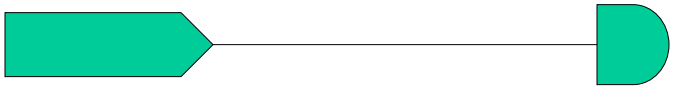
Discrete Variable QKD protocols
Lecture 2: Asymptotic key rates

Norbert Lütkenhaus

Institute for Quantum Computing, University of Waterloo

20

QKD with two non-orthogonal signals



1) send signal states
$\langle u|v\rangle = s \quad \in (0,1)$

2) perform measurements
➔observe joint probability distribution p(x,y)

3) choose test set

4) and open data for random test set:
verify observations

5) sifting: announce conclusive/inconclusive
keep conclusive results

6) key map: Alice $|u\rangle \leftrightarrow 0$
$|v\rangle \leftrightarrow 1$
Bob: determine key map results from own data

7) Alice and Bob: test p(0)=p(1)

measurements / signals		$p(\mathcal{M}_u)$ $\mathcal{M}_u$ $\|u\rangle$	$\|\bar{u}\rangle$	$p(\mathcal{M}_v)$ $\mathcal{M}_v$ $\|v\rangle$	$\|\bar{v}\rangle$
$p(u)$	$\|u\rangle$	1	0	s^2	$1-s^2$
$p(v)$	$\|v\rangle$	s^2	$1-s^2$	1	0

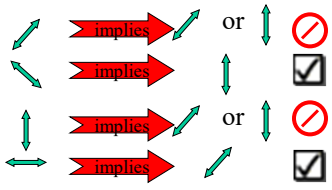
p(y|signal, measurement)
[in absence of Eve]

21

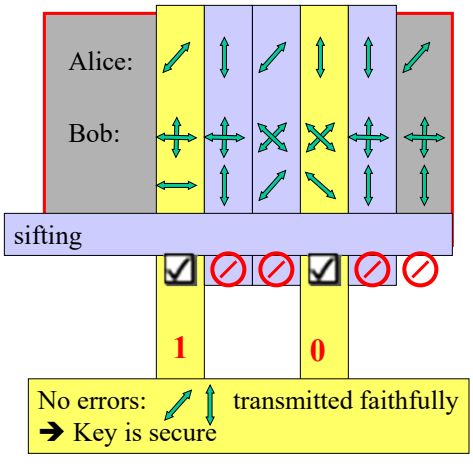
Two state protocol (B92)

Create random key:
➔random signals
➔random measurements

What Bob's measurement results tell about Alice's signals:



Public channel:
➔Bob selects events
➔Establishes advantage over Eve

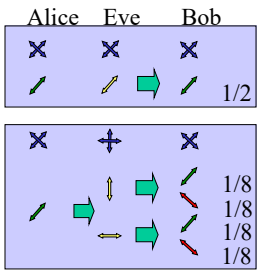


22

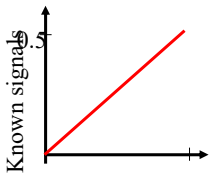
About errors …

1) There are always errors in real implementations, so
Alice and Bob need to perform error correction!

2) Eve should have negligible information on the key:



Sifted key: Right: 3/4
Wrong: 1/4



We need to cut Eve's correlation with the key: **privacy amplification!**
➔ **established classical procedure!**

23

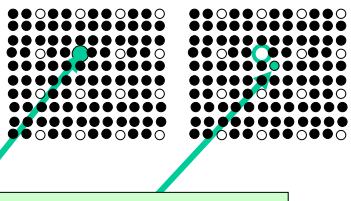
Correcting the errors

(0,1,0,0,1,0,0)➔vector

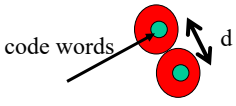
error transforms one valid sequence into another
➔ error cannot be corrected!

embed valid vectors in larger vector space:

- fill vectors (invalid sequence)



reassign invalid sequences to nearest valid sequence
➔ correct some errors with high probability

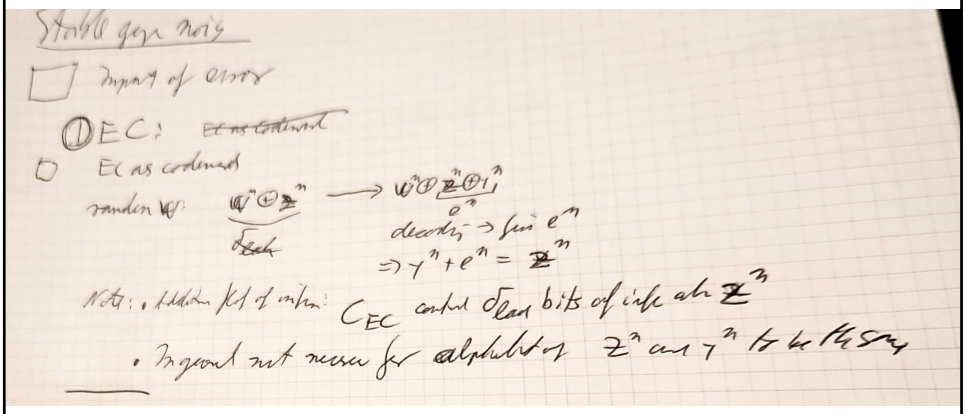


Embedding (error correction code)
[n,k,d] codes:
- takes message of length k,
- embed into codespace of n-bit strings
- protects against $\lfloor \frac{d-1}{2} \rfloor$ errors.

Shannon: (ideal error correction)
Leakage of information to Eve is H(Z|YC)
Z: result of key map
Y: Bob's measurement results
C: classical announcements

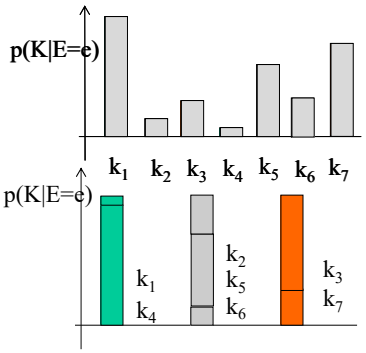
24

EC



25

Privacy Amplification: the key from Eve's point of view



key is not secret
Eve has a-priori information (correlation)
IF Alice and Bob know the distribution p(K|E=e), they can make a secret key by mapping the keys to a smaller set of keys:

Good news:

This works also without knowing the exact distribution p(K|E=e) using *universal$_2$ hash functions*

Does not work perfectly, but can be made work arbitrarily well
- for sufficiently long raw keys
- at extra cost of key length

➔ Left-over Hash Lemma

26

Left-over hash lemma
Privacy Amplification

Left-over hash lemma (structure)

Paraphrased from Renner thesis … notation details coarse grained!!!

Let $\rho_{XE'}$ be a classical register X together with a quantum system E', then applying a random hash function out of a family that maps register X to binary outputs of length l bits, then

$$\frac{1}{2}\left\| \rho_{F(X)E'} - \left(\frac{1}{2^l} \sum_{x' \in \{0,1\}^l} |x'\rangle\langle x'| \right) \otimes \rho'_E \right\|_1 \leq 2^{-\left(H(X|E')_{\rho_{XE'}} - l\right)}$$

Note: many variations possible, using different entropic measures H, with resulting factors additional terms etc

Application in QKD

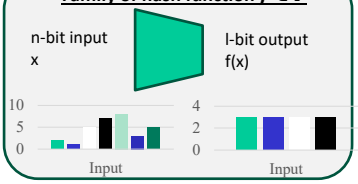
➔ To achieve

$$\frac{1}{2}||\rho^{real} - \rho^{ideal}||_1 \leq \epsilon_{sec}$$

Select the extracted key length as

$$l \leq H(X|E')_{\rho_{XE'}} - \log_2 \frac{1}{\epsilon_{sec}}$$

Family of hash function $f \in F$

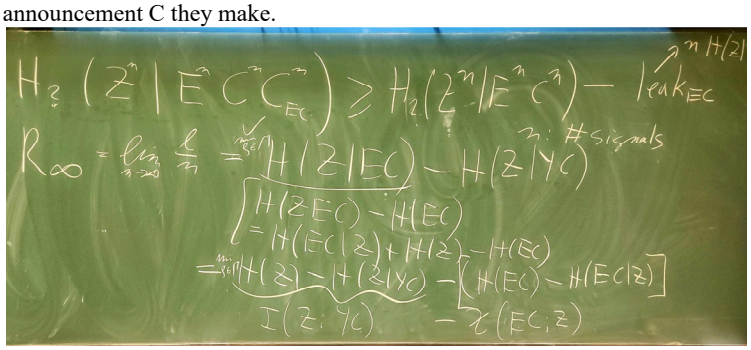


➔ Need to take minimum over all \rho_{XE'} compabible with testing observations!

27

Asymptotic key rates

The Left-over Hashing lemma will use some entropy, which is written below in the notation of the our protocol, where I explicitly denote the classical communication with respect to error correction.
It is typical to split off this communication cost first, as then the remaining quantity comes for typical protocols with tensor product form for Alice, Bob an the announcement C they make.

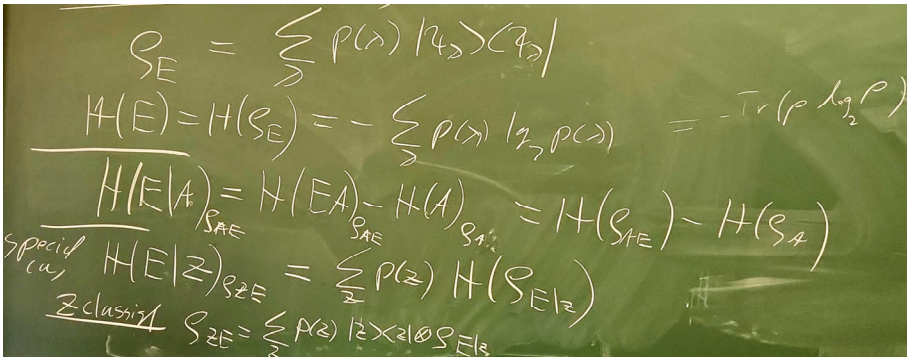


Then the asymptotic key rate (secret key per signal sent) can be expressed in terms of conditional entropies, which can be reformulated into Shannon Entropy and Holevo quantity. The last line is known as the Devetak-Winter bound

28

von Neumann Entropy

Von Neuman entropies are entropies of density matrices. We use the same symbol as Shannon entropy, as the von Neumann entropy equals to the Shannon entropy of the spectrum of rho.

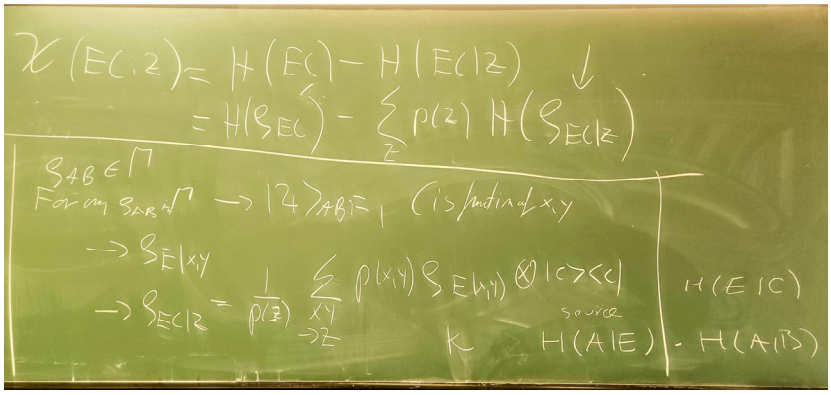


Conditional von Neumann entropies are defined via entropies of density matrices of sub-systems. They follow the same Venn type visualized relations like Shannon entropies.

Special case are conditional entropies conditioned on classical register

29

Calculating asymptotic key rates



Calculation asymptotic key rates require to calculate a Shannon information (easy) and the Holevo quantity (not trivial)
Key point is that we need to know Eve's state of knowledge (registers EC) condition on the single letter key map result z. We can do that from purifications for any state rho_AB in Gamma following our general protocol structure. The key rate is obtained by taking the worst case scenario over all density matrices rho_AB compatible with the observations.

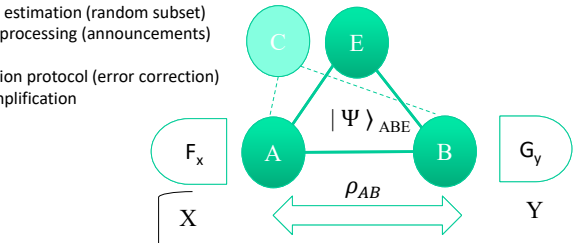
30

What can Eve know (and about what)??

[Renner, PhD Thesis 2005]

Protocol outline:

- quantum signal distribution
- quantum measurements
- Parameter estimation (random subset)
- Blockwise processing (announcements)
- Key map
- reconciliation protocol (error correction)
- Privacy Amplification



Key map: {X, C} → Z

C

frequency in tested signals: p(x,y)

$\rho \in \Gamma = \{\rho_{AB} \ |Tr[F_x \otimes G_y \ \rho_{AB}] = p(x,y)\}$

announcements C

31

Gain formula BB84 protocol

[Mayers; Shor, Preskill;Renner]

The gain formula gives the number of secure bits after error correction and privacy amplification per signal sent by Alice:

$$R_\infty = \frac{1}{2}(1 - h(e) - h(e))$$

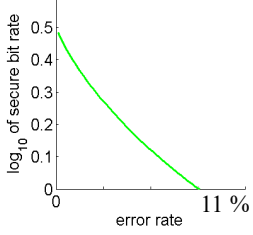
leaked information during **error correction**

e: average error rate over four signals

$h(e) := -e \log_2 e - (1-e)\log_2(1-e)$

privacy amplification

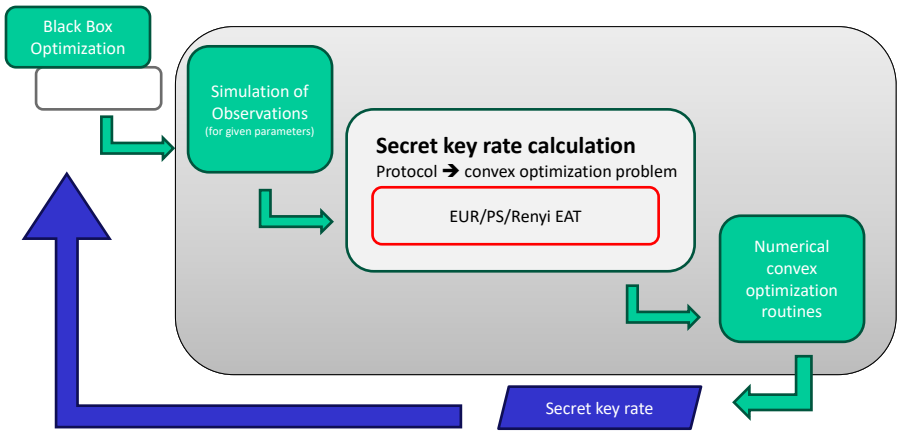
(Eve's information gain interaction with signals)



32

Open Source Software

www.openqkdsecurity.org



33

Considerations for Choice of Proof Technique

Mathematical aspects:

1. How tight a key rate do we get?
2. How does it work with protocol variations (sequence of announcements)
   - Flexibility
   - Modularity
3. Can it be extended to more detailed model assumptions (side-channels)?
4. How hard is it to calculate the key rates?

Perception aspects:

- Modularity of proof (breaking down into parts)
- Peer review due diligence
- Accessibility for evaluators not trained in quantum mechanics

34

Handling Protocol Variations

There are many protocol variations which might not be compatible with particular security proofs

- Active or passive basis choices
- Testing round: random for each round, or random subset of all signals of given length
- Announcements: on the fly, or at end of the protocol
- Classical Error Correction Announcements: encrypted of open
- Execute random permutations of signals
- Processing of multi-click events in detectors

35

Implementation Security: Side-channels

There are many side-channels and imperfections known
- Trojan Horse attack
- Incomplete dephasing of signals
- Detectors with individual detection inefficiency

➔ Try to reduce modelling assumptions in security proofs e.g. device independent QKD
➔ Do refined models to cover imperfections

There will be always gaps between model and implementation

➔ **Implementations** can never be **provable** secure!

36

Overview over Security Proof techniques

Phase error correction approach. (NO LHL)
(Koashi, 2005; Koashi 2009)

Guarantees that QECC/entanglement purification would have cut Eve out of the secret key ➔ bit and phase error estimation.

Privacy Amplification (Leftover Hashing Lemma)

(Dupuis, 2023; Renner, 2005; Tomamichel and Leverrier, 2017)

Requires estimation of Eve's knowledge based on accepted observation, via bounding entropies.

Entropic Uncertainty Relations
(bit and phase error estimation)
(Tomamichel and Renner, 2011)

Entropy Accumulation
(Arqand and Tan, 2025; Dupuis et al., 2020; Fawzi et al., 2025; Metger et al., 2022).

Postselection technique
(via IID reduction)
(Christandl et al., 2009; Nahar et al., 2024)

Both are "phase-error" based techniques : Require bounding of error rates of virtual measurements.

Equivalent upto trivial factors: (Tsurumaru, 2020)

Is best viewed as a reduction to IID. Any analysis can be used for IID

37

37

arXiv > quant-ph > arXiv:2502.10340

Quantum Physics

[Submitted on 14 Feb 2025 (v1), last revised 16 May 2025 (this version, v2)]

QKD security proofs for decoy-state BB84: protocol variations, proof techniques, gaps and limitations

Devashish Tupkary, Ernest Y.-Z. Tan, Shlok Nahar, Lars Kamin, Norbert Lütkenhaus

	Entropic Uncertainty	Phase Error	PS/Quantum DeFinetti technique	Entropy Accumulation
Performance	Good	Good	Pessimistic	Good
Robustness against imperfections	Robust against *Independent* imperfections	Robust against *Independent* imperfections	Robust against *IID* imperfections	Robust against *Independent* imperfections
Peer Review Scrutiny	High	High	High	Low (recent)
Modularity for extensions/modifications	Low	Low	High	High
Accessibility	High	Less modular	High	Medium
Protocol Choices	Can be a challenge	Can be a challenge	Can be a challenge (permutation requirement)	Medium
Computability of Key rates	Easy (Analytic formula)	Easy (Analytic Formula)	Medium (needs numerics)	High (needs more involved numerics)

38

Key Rates are Security Proof dependent

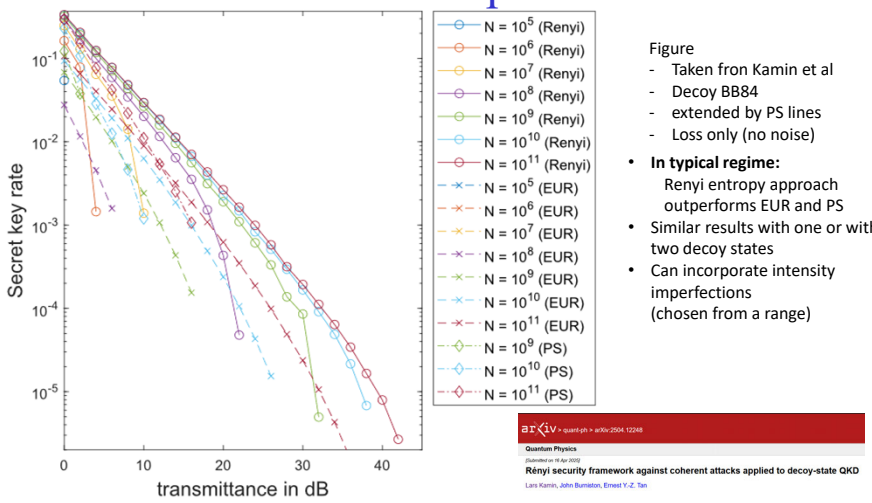


Figure
- Taken fron Kamin et al
- Decoy BB84
- extended by PS lines
- Loss only (no noise)

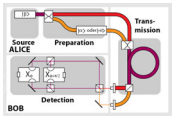
- **In typical regime:** Renyi entropy approach outperforms EUR and PS
- Similar results with one or with two decoy states
- Can incorporate intensity imperfections (chosen from a range)

39

Protocol vs Implementation security

Actual Device
e.g. reality based

modelling



Quantum Optical Model
e.g. mode based

$||\rho_{ABE} - \rho_{AB} \otimes \rho_C||_1 \leq \epsilon$

Security Proof

Protocol Security
(rigorous math …)

Implementation Security
(best practice …)

40

Wha… …oof?

Boundary between scientific and acceptance can be moved (device independent security proofs) but never vanishes

Testing of Models
e.g. by embedding into larger models
- requires experience based cut-off
➔no scientific proof possible

-Model of Devices
-e.g. QM description
-quantum security perimeter

So what remains?
QKD provides secret key that is future-proof (quantum part):
the key is as secure for all future as it is at its creation!

➔need to find common level of acceptance (ETSI standardization) (testable/quantifyable or not)

-security parameters

Softwar…
-verified
(development & execution)
-hardware security perimeter
- key management

- Scientific Security Proof
"perfect secret key with exception of probability ^{2}"

Security proof defined by scientific standard

41

Protocol Security Status

What people hear (short version)
"There are no full security proofs of QKD"

Position Paper on
Quantum Key Distribution

French Cybersecurity Agency (ANSSI)
Federal Office for Information Security (BSI)
Netherlands National Communications Security Agency (NLNCSA)
Swedish National Communications Security Authority, Swedish Armed Forces

What the France/Sweden/Netherlands/Germany Position paper says:

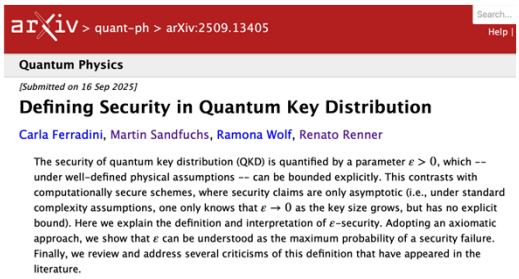
"QKD security proofs
… QKD protocols can provide security based on quantum-physical principles without requiring assumptions about the hardness of mathematical problems. … A security proof should describe the QKD protocol in a precise mathematical model with well-stated assumptions, and derive a precise statement expressing and quantifying the security of the protocol in this model. In order for a security proof, which is purely theoretical and conducted in an abstract model, to relate to the security of an actual implementation in a meaningful way, the security statement should be proved in a model that reflects realistic conditions as much as possible.
…
However, to the best of our knowledge, no security proof for a practically relevant protocol has been written up in a cohesive and comprehensive way that satisfies the requirements outlined above. "

➔In short: there is no scientific reference available which gives a self-contained mathematical security proof for a practical protocol
➔It does not mean that there are doubts that such a paper can be written …

42

Our answer (Part 1/3)

Explain and justify composable security definition (ETH Zurich).



arXiv > quant-ph > arXiv:2509.13405

Search... Help

Quantum Physics

[Submitted on 16 Sep 2025]

Defining Security in Quantum Key Distribution

Carla Ferradini, Martin Sandfuchs, Ramona Wolf, Renato Renner

The security of quantum key distribution (QKD) is quantified by a parameter $\varepsilon > 0$, which -- under well-defined physical assumptions -- can be bounded explicitly. This contrasts with computationally secure schemes, where security claims are only asymptotic (i.e., under standard complexity assumptions, one only knows that $\varepsilon \to 0$ as the key size grows, but has no explicit bound). Here we explain the definition and interpretation of ε-security. Adopting an axiomatic approach, we show that ε can be understood as the maximum probability of a security failure. Finally, we review and address several criticisms of this definition that have appeared in the literature.

43

Our answer (Part 2/3)

1. Reviews key elements of security proofs.
2. ***Focus is on gaps, limitations, common mistakes in existing literature.***
3. Reviews all existing proofs for decoy-state BB84 + compares different aproaches.

arXiv > quant-ph > arXiv:2502.10340

Search... Help

Quantum Physics

[Submitted on 14 Feb 2025 (v1), last revised 16 May 2025 (this version, v2)]

QKD security proofs for decoy-state BB84: protocol variations, proof techniques, gaps and limitations

Devashish Tupkary, Ernest Y.-Z. Tan, Shlok Nahar, Lars Kamin, Norbert Lütkenhaus

We review the current status of security proofs for practical decoy-state Quantum Key Distribution using the BB84 protocol, focusing on optical implementations with weak coherent pulses and threshold photodetectors. The primary aim of this review is to highlight gaps in the existing literature. Such gaps may arise, for instance, from mismatches between detailed protocol specifications and proof technique elements, reliance on earlier results based on different assumptions, or protocol choices that overlook real world requirements. While substantial progress has been made, our overview draws attention to the details that still demand careful attention.

44

Our answer (Part 3/3)

1. ***Very generic***: Core protocol has abstract elements : Different specification yield different protocols. Only change is numerical computation of key rates.

2. No imperfections yet, but many tools already exist, and there is clear path forward to incorporate them!

3. Tight key rates!

arXiv > quant-ph > arXiv:2601.18035

Quantum Physics

[Submitted on 25 Jan 2026]

A rigorous and complete security proof of decoy-state BB84 quantum key distribution

Devashish Tupkary, Shlok Nahar, Amir Arqand, Ernest Y.-Z. Tan, Norbert Lütkenhaus

We present a rigorous and complete security proof of the decoy-state BB84 quantum key distribution (QKD) protocol. Our analysis aims to achieve a high standard of mathematical rigour and completeness, thereby providing the necessary foundation for certification and standardization efforts. Beyond establishing the security of a specific protocol, this work develops a general and modular framework that can be readily adapted to a broad class of QKD protocols, including both prepare-and-measure and entanglement-based variants. Our framework unifies all major ingredients required for the analysis of realistic QKD protocols, including the analysis of classical authentication and classical processing, source-replacement schemes, finite-size analysis, source maps, squashing maps, and decoy-state techniques. In doing so, this work consolidates a diverse range of techniques scattered across the QKD literature into a unified formalism, representing a general and rigorous treatment of QKD security. Finally, it outlines a clear path towards incorporating practical imperfections within the same framework, thereby laying the groundwork for addressing implementation security in future analysis.

arXiv > quant-ph > arXiv:2504.20417

Quantum Physics

[Submitted on 29 Apr 2025 (v1), last revised 26 May 2025 (this version, v3)]

Protocol-level description and self-contained security proof of decoy-state BB84 QKD protocol

Akihiro Mizutani, Toshihiko Sasaki, Go Kato

45